Sein Analytics

Type 2 SOC 2

2022

REPORT ON SEIN ANALYTICS’ DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS RELEVANT TO SECURITY AND CONFIDENTIALITY

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

July 1, 2021 to June 30, 2022

Table of Contents

SECTION 1

ASSERTION OF SEIN ANALYTICS MANAGEMENT

ASSERTION OF SEIN ANALYTICS MANAGEMENT

September 8, 2022

We have prepared the accompanying description of Sein Analytics' ('Sein' or 'the Company') Trading and Asset Management Platform Services System titled "Sein Analytics' Description of Its Trading and Asset Management Platform Services System throughout the period July 1, 2021 to June 30, 2022" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the Trading and Asset Management Platform Services System that may be useful when assessing the risks arising from interactions with Sein's system, particularly information about system controls that Sein has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Confidentiality (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*).

Sein 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 Sein, to achieve Sein's service commitments and system requirements based on the applicable trust services criteria. The description presents Sein Analytics' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Sein'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 Sein, to achieve Sein's service commitments and system requirements based on the applicable trust services criteria. The description presents Sein's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Sein's controls.

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

a. the description presents Sein Analytics' Trading and Asset Management Platform Services System that was designed and implemented throughout the period July 1, 2021 to June 30, 2022, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period July 1, 2021 to June 30, 2022, to provide reasonable assurance that Sein'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 Sein's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period July 1, 2021 to June 30, 2022, to provide reasonable assurance that Sein'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 Sein's controls operated effectively throughout that period.

Samuel Belu-John

Samuel Belu-John
Co-Founder and Lead Developer
Sein Analytics

SECTION 2

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Sein Analytics

Scope

We have examined Sein Analytics' accompanying description of its Trading and Asset Management Platform Services System titled "Sein Analytics' Description of Its Trading and Asset Management Platform Services System throughout the period July 1, 2021 to June 30, 2022" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period July 1, 2021 to June 30, 2022, to provide reasonable assurance that Sein Analytics' service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Confidentiality (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*).

Sein 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 Sein Analytics, to achieve Sein's service commitments and system requirements based on the applicable trust services criteria. The description presents Sein's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Sein'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 Sein, to achieve Sein's service commitments and system requirements based on the applicable trust services criteria. The description presents Sein's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Sein'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

Sein 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 Sein's service commitments and system requirements were achieved. Sein has provided the accompanying assertion titled "Assertion of Sein Analytics Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Sein 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 Sein Analytics' Trading and Asset Management Platform Services System that was designed and implemented throughout the period July 1, 2021 to June 30, 2022, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period July 1, 2021 to June 30, 2022, to provide reasonable assurance that Sein'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 Sein's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period July 1, 2021 to June 30, 2022, to provide reasonable assurance that Sein'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 Sein'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 Sein, user entities of Sein Analytics' Trading and Asset Management Platform Services System during some or all of the period July 1, 2021 to June 30, 2022, business partners of Sein subject to risks arising from interactions with the Trading and Asset Management Platform Services System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

A-LIGN ASSURANCE

Tampa, Florida
September 8, 2022

SECTION 3

SEIN ANALYTICS' DESCRIPTION OF ITS TRADING AND ASSET MANAGEMENT PLATFORM SERVICES SYSTEM THROUGHOUT THE PERIOD JULY 1, 2021 TO JUNE 30, 2022

OVERVIEW OF OPERATIONS

Company Background

Sein Analytics was founded by Samuel Belu-John and Anne Clark with the goal of combining Samuel's skills in application development with Anne's skills in design and user experience. From the start, their goal was to build a financial technology company specifically focused on markets that are underserved with respect to data processing and analytics.

After extensive user research, they realized that Credit Unions and Community Banks had a real need in executing loan transactions.

Specifically, their research revealed that most of these institutions did not know the bid/ask spread when transacting. These institutions also spent unnecessary funds on data rooms/storage and analytic tools when attempting to transact with each other.

Description of Services Provided

Sein's application completely digitizes the process for these institutions and provides the following advantages:

- Go to market and application release were pushed back pending a second SOC 2 Type 2 audit to account for significant changes in application deployment and configuration
- Secure real-time pricing market with in-depth details and key statistics at the pool and loan level
- Real-time e-mail notifications every time a bid is submitted
- Digital process flow from bidding to document submission and execution using the HelloSign plugin
- Built-in agile loan-level due diligence module where buyers can raise issues and pose questions at the loan and document level
- Advanced loan-level cash flow analytics

Application security is enhanced using the following third-party tools and encryption methods:

- OPSWAT Via Cloudinary Digital Asset Management (DAM)- to scan all user submitted documents for malware and viruses before they are stored on cloud storage and made available to other members
- Cloudinary Digital-Asset-Management has been fully incorporated into the system application for the storage and retrieval of customer sensitive documents
- ip2location - to restrict access only to users with valid IP addresses
- inspector.io - to monitor and notify the Sein team of application errors and user http requests
- Twillo/Authy for two-factor authentication
- S3 AES-256 file encryption at rest
- Database encryption at rest
- PDFTron Web Viewer has been integrated within the application to enable users to read and modify documents within the application
- To enable faster build of the front-end application we've fully integrated several Syncfusion libraries into the application

Principal Service Commitments and System Requirements

Sein Analytics designs its processes and procedures related to Trading and Asset Management Platform Services to meet its objectives for its Trading and Asset Management Platform Services. Those objectives are based on the service commitments that Sein Analytics makes to user entities, the laws and regulations that govern the provision of Trading and Asset Management Platform Services, and the financial, operational, and compliance requirements that Sein Analytics has established for the services.

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 Trading and Asset Management Platform Services 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

Sein establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Sein'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 Trading and Asset Management Platform Services.

Components of the System

Infrastructure

Primary infrastructure used to provide Sein Analytics' Trading and Asset Management Platform Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Virtual Private Cloud (VPC)	Amazon Web Services (AWS)	This virtual network closely resembles a traditional network that you'd operate in your own data center
Route 53	AWS	Reliable way to route end users to Internet applications by translating site names into numeric IP addresses
Amazon WAF	AWS	Web application firewall that helps protect your web applications or APIs against common web exploits that may affect availability, compromise security, or consume excessive resources
Load Balancing	AWS	Distributes incoming application traffic across multiple targets, such as EC2 instances, in multiple Availability Zones. This increases the availability of your application
Internet Gateway	AWS	Provide a target in your VPC route tables for Internet-routable traffic and perform network address translation (NAT) for instances that have been assigned public IPv4 addresses
EC2 Instance	AWS	Provides scalable computing capacity in AWS. You can launch as many or as few virtual servers as you need, configure security and networking, and manage storage
Amazon ECR	AWS	Fully managed Docker container registry that makes it easy for developers to store, manage, and deploy Docker container images

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Relational Database Service (RDS)	AWS	Amazon RDS handles routine database tasks such as provisioning, patching, backup, recovery, failure detection, and repair. This managed relational database service provides you six familiar database engines
Auto Scaling	AWS	Monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost
Amazon S3	AWS	Amazon S3 has a simple web services interface that you can use to store and retrieve any amount of data, at any time, from anywhere on the web
Amazon ECS	AWS	Highly scalable, fast, container management service that makes it easy to run, stop, and manage Docker containers on a cluster
Elasticache (REDIS)	AWS	Web service that makes it easy to set up, manage, and scale a distributed in-memory data store or cache environment in the cloud. It provides a high-performance, scalable, and cost-effective caching solution
DocumentDB	AWS	Fast, scalable, highly available, and fully managed document database service that supports MongoDB workloads
Amazon CloudWatch	AWS	Provides the Sein team with data and actionable insights to monitor applications, respond to system-wide performance changes, optimize resource utilization, and receive a unified view of operational health
Lambda	AWS	Run code for virtually any type of application or backend service - all with zero administration. You can set up your code to automatically trigger from other AWS services or call it directly from any web or mobile app
Amazon SNS	AWS	Highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and serverless applications

Software

Primary software used to provide Sein Analytics' Trading and Asset Management Platform Services System includes the following:

Primary Infrastructure		
Infrastructure	**Type**	**Purpose**
Docker	Same Linux kernel as the host machine	Designed to make it easier to create, deploy, and run applications by using containers. Containers allow a developer to package up an application with all of the parts it needs, such as libraries and other dependencies, and deploy it as one package

Primary Infrastructure		
Infrastructure	**Type**	**Purpose**
Falco	Linux	Falco detects unexpected application behavior and alerts on threats at runtime
Slack	Not appliable	Unifies systems and sends and receives notifications
MySQL Aurora	Linux	Fully managed, MySQL-compatible, relational database engine. Aurora MySQL is a drop-in replacement for MySQL and makes it simple and cost-effective to set up, operate, and scale your new and existing MySQL deployments
Bastion AMI	Canonical, Ubuntu,16.04 LTS, amd64 xenial image build on 2019-06-28	AMI provides the information required to launch an instance. You must specify an AMI when you launch an instance
Cluster AMI	Amazon Linux AMI 2018.03 ECS	AMI provides the information required to launch an instance. You must specify an AMI when you launch an instance
AWS CodePipeline	Not applicable	Fully managed continuous delivery service. CodePipeline automates the build, test and deploy phases of their release process. Integrates seamlessly with their GitHub versioning
Node.js Version 10	Alpine Linux (Docker)	JavaScript runtime environment that executes JavaScript code outside of a browser
NGINX	Alpine Linux (Docker)	High-performance HTTP server and reverse proxy. NGINX is known for its high performance, stability, rich feature set, simple configuration, and low resource consumption
PHP Version 8.1	Debian (Docker)	Server-side dynamic scripting language, and a powerful tool for building web applications. The latest release of PHP comes complete with its own production ready server. This is not used in production
VUEJS	JavaScript/Node.js	Powerful web framework for building single page applications. We are still in the process of completely migrating to VueJS. As part of the preparation work for release of the application they have completely decoupled the backend and frontend into two separate applications
Laravel Framework	PHP Framework	Laravel is a free, open-source PHP web framework intended for the development of web applications following the model-view-controller architectural pattern. We continue to deepen their integration with

People

Sein key personnel and roles are as follows:

Samuel Belu-John - Lead Developer and Co-Founder:

- Produce all back-end and front-end code according to user experience and design specifications
- Manage code repository security and access
- Manage primary cloud provider account security and access
- Develop application key components and configurations
- Manage vendor relations and business development

- Create key organization policies and procedures
- Ensure implementation of security protocols in coordination with Lead DevOps Engineer
- Ensure all policies and procedures are implemented and adhered to in coordination with the Operations and Business Development Analyst
- Direct management and maintenance for all ticketing system boards associated with code deployment and changes to the SaaS application

Anne Clark - Head of Product Design and Co-Founder:

- Develop and update SaaS application user experience (UX) and design
- Approves all policies and procedures and their implementation
- Ensures compliance with policies and procedures in coordination with the Lead Developer, Operations, and Business Development Analyst
- Design and oversee the production of all marketing and business development materials, including but not limited to (brochures, trade show graphics, pamphlets, business cards, and logos)
- Manages and maintains corporate account and business cards
- Manages overall budgeting and approves all corporate expenses
- Manages product quality control/assurance and maintains documentation of UX/Design changes and updates
- Direct responsibility for managing and maintaining all ticketing system boards associated with
- QA/QC, UX/Design, and Marketing

Anne currently serves as the organization's interim CFO and Lead-COO. Sein is actively searching for someone to permanently take over the CFO role. Anne is responsible for ensuring that all policies and procedures implemented meet minimum basic standards and in accordance with their stated values and principles.

Thiago Maior - Lead DevOps Engineer:

- Manages AWS infrastructure DevOps team
- Directs the implementation of SaaS infrastructure and security configurations
- Ensures infrastructure and security configurations adhere to all policies and procedures
- Leads the maintenance and monitoring of key application systems and security protocols
- Manages maintenance and ensures proper documentation of key system configurations
- Leads weekly standup DevOps meetings and ensures that all key issues are properly reflected in the ticketing systems DevOps board
- Directs the assignment of resources required to maintain and implement infrastructure configurations and maintenance
- Responsible for managing and maintaining all ticketing system boards associated with DevOps, infrastructure monitoring and updates

Thiago works with Sein as a third-party vendor in the role as CIO. Thiago is responsible for the integrity of the application infrastructure, monitoring and maintenance. In this role, Thiago and his team work closely and in tandem with the Lead Developer.

As they work towards the final release of the application, we've decided to deepen their relationship with EZOps. We've signed a three-month contract whereby EZOps will also help in the development of the remaining frontend and backend of the application systems.

Data

Data as defined by Sein:

- Market seller loan tape and any subsequent updates to the loans during the transaction period - Structured Query
- Loan documents for market buyers to conduct due diligence prior to final agreement - AWS S3 simple storage

- User profile data - Stored on both SQL and S3
- User contract documents - S3 and HelloSign API

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

Physical Security

As a cloud-based remote company, Sein does not currently maintain a permanent physical office. The company does all its work using cloud-based applications to share documents and collaborate in the development and implementation of the information system/application. The primary purpose of the Physical Security Procedures is to specify minimum requirements for employees' and independent contractors' physical locations (e.g., home office, apartment, co-working spaces) and provide guidance for connectivity to cloud-based applications and the physical security of laptops and personal computers.

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 system.

Logical Access

For the SaaS application Sein:

1. Requires that each user log on to the information system from only one IP address at a time, this prevents multiple logins with the same credentials.
2. Requires that all users have a smart phone with multi-factor authentication enabled, specifically, access codes are sent via the Authy API.
3. Requires that users log out when not actively using the information system. This is automatically enforced, by forcibly logging out the user after 5 minutes of inactivity.
4. Monitors user duration/usage of the information system.
5. User must be using a valid IP address as the system will refuse IP addresses via VPN or other IP masking tools.

For internal systems and third-party applications:

1. Limited access is granted to freelancers/independent contractors and third-party providers on an as-needed basis.
2. Permissions and access to development environment is controlled via AWS IAM (we are currently moving Samuel's local development environment to AWS Cloud9).

Computer Operations - Backups

Sein is a completely cloud-based company, as such, data backup and replication are handled by one of either AWS, GitHub, Google Drive/Gmail (forwarded from MediaTemple) or MediaTemple. The company does not maintain its own on-site backup media tapes. All customer data is stored in the cloud on one of AWS S3 or AWS RDS.

Computer Operations - Availability

Sein has developed an incident response policy and procedures manual that covers all information security incidents and breaches. The incident response policy provides a defined, organized approach for handling any potential threats to the information system/application and data, as well as the appropriate actions to be taken when the source of the intrusion or incident is traced to Sein virtual private network (VPN).

The policy identifies and describes the roles and responsibilities of the Incident Response Team (IRT), who oversee incident response and management.

Incidents include, but are not limited to, the following:

- Breach of personal information
- Unauthorized distribution of IT asset verbally, in writing, or electronically
- Virus or other malware infection
- Firewall breach
- Use of unapproved or unlicensed software on the information system/application
- Accessing information database or storage with someone else’s authorization
- Printing or copying confidential information and not storing it correctly or confidentially

Change Control

Sein has developed a change management policy manual to guide the implementation and documentation of infrastructure and application changes. This includes a robust system of approvals and Q&A procedures that must be adhered to prior to a deployment or implementation.

Changes to the information system or application may arise from many circumstances, such as:

- Periodic Maintenance
- User Requests
- Acquisition of new hardware and/or software
- Hardware and/or software upgrades
- Changes or modification to the infrastructure
- Unforeseen events
- Database change
- Infrastructure change

For application and infrastructure changes, Sein uses a version control repository (GitHub) that maintains a history of code changes to support rollback capabilities and track changes to developers.

Data Communications

The entire Sein application infrastructure is built within an AWS VPC. All AWS EC2 instances are behind private subnets with access to the Internet trafficked via a NAT gateway. Sein infrastructure is deployed using InfrastructureCode with AWS CloudFormation and Jenkins coordinating which services are launched and how the various components communicate with each other. Redundancy is built into the system through replication of the S3 simple storage and the main application database across multiple AWS availability zones.

An intrusion detection monitoring system, Falco, has been deployed within the architecture and notifies the Sein team of any unexpected intrusion or activity within the VPC. An S3 File integrity monitoring system has also been deployed within the architecture and notifies the Sein team of any access to or changes in customer loan documents stored in S3 buckets. Vulnerability scans are performed regularly with third-party vendors CloudSploit and Intruder.io. Further Intruder.io does an automated penetration testing of the application and infrastructure with each scan.

Boundaries of the System

The scope of this report includes the Trading and Asset Management Platform Services System performed at the Brooklyn, New York facility.

This report does not include the cloud hosting services provided by AWS at its regionally hosted 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 Sein's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Sein'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 acknowledgement 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

Sein'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

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

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

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

Organizational Structure and Assignment of Authority and Responsibility

Sein’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.

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

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

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

Human Resource Policies and Practices

Sein’s success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Sein’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

The Sein risk management system identifies the risks it faces and puts measures in place to manage those risk. In managing risk, it is the company’s practice to take advantage of potential opportunities while managing potential adverse effects.

The company risk register assigns ownership and responsibility for each identified risk, to a specified risk owner.

Sein’s risk assessment matrix is used as the benchmark in planning and implementing risk management measures. It takes into consideration the nature, scale and complexity of the business.

Sein’s risk assessment has identified 9 ‘Key Risks’:

- Loss or theft of intellectual property
- Compliance violations and regulatory actions
- Loss of control over end user actions
- Malware infections that unleash a targeted attack
- Contractual breaches with customers or business partners
- Diminished customer trust
- Data breach requiring disclosure and notification to victims
- Increased customer churn
- Revenue losses

Integration with Risk Assessment

The environment in which the system operates, the commitments, agreements, and responsibilities of Sein Analytics’ Trading and Asset Management Platform Services system; as well as the nature of the components of the system result in risks that the criteria will not be met. Sein 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, Sein’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

As a cloud based remote company, Sein does not currently maintain a permanent physical office. The company does all its work using cloud based applications to share documents and collaborate in the development and implementation of the information system/application and to conduct normal business operations.

While the team is still relatively small in size, an advanced suite of tools is maintained that are used to handle information and communication within the relevant systems, with many tools either partially or fully integrated with one another.

Sein primarily relies on the use of Trello/Jira, Google Drive, and Slack to conduct day to day business operations. All company tasks are managed using the Trello/Jira Agile Tracking Software, all company documents are stored using Google Drive, and work-related communication is sent through Slack.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Sein’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, regular evaluations, or a combination of the two.

On-Going Monitoring

Sein’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 Sein’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 Sein’s personnel.

Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of ongoing 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 Security and Confidentiality criteria were applicable to the Sein Analytics Trading and Asset Management Platform Services system.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS at their regional facilities.

Subservice Description of Services

AWS provides cloud hosting services that include but are not limited to high system availability and environmental protections surrounding the Sein production environment.

Complementary Subservice Organization Controls

Sein’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 the trust services criteria related to Sein’s services to be solely achieved by Sein control procedures. Accordingly, the subservice organization, in conjunction with the services, should establish their own internal controls or procedures to complement those of Sein.

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

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Security	CC6.4	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.

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

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

COMPLEMENTARY USER ENTITY CONTROLS

Sein'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 Sein's services to be solely achieved by Sein control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Sein'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 Sein.
2. User entities are responsible for notifying Sein of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Sein 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 Sein services.

6. User entities are responsible for providing Sein with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Sein of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

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

Confidentiality
Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel. Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

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

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

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

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

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

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Core values are communicated from executive management to personnel through policies, directives, guidelines, the code of conduct, and the employee handbook.	Inspected the employee handbook, code of conduct policies and procedures, information security policies and procedures, and the entity's shared drive to determine that core values were communicated from executive management to personnel through policies, directives, guidelines, the code of conduct, and the employee handbook.	No exceptions noted.
		An employee handbook and code of conduct are documented to communicate workforce conduct standards and enforcement procedures.	Inspected the employee handbook and code of conduct policies and procedures to determine that an employee handbook and code of conduct were documented to communicate workforce conduct standards and enforcement procedures.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.	Inquired of the Lead Developer regarding new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
			Inspected the employee handbook and code of conduct acknowledgment template to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the signed employee handbook and code of conduct acknowledgment for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	Testing of the control activity disclosed that no new employees were hired during the review period.
		Upon hire, personnel are required to complete a background check.	Inquired of the Lead Developer regarding background checks to determine that upon hire, personnel were required to complete a background check.	No exceptions noted.
			Inspected the background check policy to determine that upon hire, personnel were required to complete a background check.	No exceptions noted.
			Inspected the completed background check for a sample of new hires to determine that upon hire, personnel were required to complete a background check.	Testing of the control activity disclosed that no new employees were hired during the review period.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
		Sanction policies, which include probation, suspension, and termination, are in place for employee misconduct.	Inspected the code of conduct policies and procedures to determine that sanction policies, which include probation, suspension, and termination, were in place for employee misconduct.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		An anonymous hotline is in place to allow employees, third-parties and customers to report unethical behavior in a confidential manner.	Inspected the anonymous hotline to determine that an anonymous hotline was in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	No exceptions noted.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Executive management maintains independence from those that operate the key controls within the environment.	Inspected the organizational chart 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 with operational management to assess the effectiveness and performance of internal controls within the environment.	Inspected the annual meeting minutes to determine that executive management met weekly with operational management to assess the effectiveness and performance of internal controls within the environment.	No exceptions noted.
		Operational management assigns responsibility for and monitors the effectiveness and performance of internal controls implemented within the environment.	Inspected the internal controls matrix to determine that operational management assigned responsibility for and monitored the effectiveness and performance of internal controls within the environment.	No exceptions noted.
			Inspected the annual meeting minutes to determine that operational management assigned responsibility for and monitored the effectiveness and performance of internal controls within the environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority.	No exceptions noted.
		Executive management reviews the organizational chart annually and makes updates to the organizational structure and lines of reporting, if necessary.	Inspected the revision history of the organizational chart to determine that executive management reviewed the organizational chart annually and made updates to the organizational structure and lines of reporting, if necessary.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's shared drive site.	Inspected the job description for a sample of job roles and the entity's shared drive site to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's shared drive site.	No exceptions noted.
		Executive management reviews job descriptions annually and makes updates, if necessary.	Inspected the revision history for a sample of job descriptions to determine that executive management reviewed job descriptions annually and made updates, if necessary.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.	Inquired of the Lead Developer regarding new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct which requires adherence to the personnel’s job role and responsibilities.	No exceptions noted.
			Inspected the employee handbook and code of conduct acknowledgement template to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct which requires adherence to the personnel’s job role and responsibilities.	No exceptions noted.
			Inspected the signed employee handbook and code of conduct acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct which requires adherence to the personnel’s job role and responsibilities.	Testing of the control activity disclosed that no new employees were hired during the review period.
		Executive management has established proper segregation of duties for key job functions and roles within the organization.	Inspected the organizational chart, internal controls matrix, and a sample of job descriptions to determine that executive management established proper segregation of duties for key job functions and roles within the organization.	No exceptions noted.

<table>
<tr><th colspan="5">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="5">Control Environment</th></tr>
<tr><th>CC1.0</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td></td><td></td><td>Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's shared drive site.</td><td>Inspected a sample of job descriptions and the entity's shared drive to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's shared drive site.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third-parties.</td><td>Inspected the vendor management policies and procedures to determine that a vendor risk assessment was required on an annual basis.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third-parties.</td><td>Inspected the completed vendor risk assessment to determine that a vendor risk assessment was performed on an annual basis which included reviewing the activities performed by third-parties.</td><td>No exceptions noted.</td></tr>
<tr><td>CC1.4</td><td>COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.</td><td>Policies and procedures are in place that outline the performance evaluation process.</td><td>Inspected the employee performance evaluation document to determine that policies and procedures were in place that outlined the performance evaluation process.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>Performance and conduct evaluations are performed for personnel on an annual basis.</td><td>Inspected the performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.</td><td>No exceptions noted.</td></tr>
</table>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer process.	Inquired of the Lead Developer regarding new hires to determine that job requirements were documented in the job descriptions and candidates' abilities to meet these requirements were evaluated as part of the hiring or transfer process.	No exceptions noted.
			Inspected the hiring and recruiting policy to determine that job requirements were documented in the job descriptions and candidates' abilities to meet these requirements were evaluated as part of the hiring or transfer process.	No exceptions noted.
			Inspected the job description for a sample of job roles to determine that job requirements were documented in the job descriptions and candidates' abilities to meet these requirements were evaluated as part of the hiring or transfer process.	Testing of the control activity disclosed that no new employees were hired during the review period.
		Executive management has created a training program for its employees.	Inspected the information security and awareness training modules to determine that executive management created a training program for its employees.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity assesses training needs on an annual basis.	Inspected the information security and awareness training module and the training certificate for a sample of current employees to determine that the entity assessed the training needs on an annual basis.	No exceptions noted.
		Upon hire, personnel are required to complete a background check.	Inquired of the Lead Developer regarding background checks to determine that upon hire, personnel were required to complete a background check.	No exceptions noted.
			Inspected the background check policy to determine that upon hire, personnel were required to complete a background check.	No exceptions noted.
			Inquired of the Lead Developer regarding background checks to determine that upon hire, personnel were required to complete a background check.	Testing of the control activity disclosed that no new employees were hired during the review period.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's shared drive site.	Inspected a sample of job descriptions and the entity's shared drive to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's shared drive site.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.	Inquired of the Lead Developer regarding new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct which required adherence to the personnel’s job role and responsibilities.	No exceptions noted.
			Inspected the employee handbook and code of conduct acknowledgement template to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct which required adherence to the personnel’s job role and responsibilities.	No exceptions noted.
			Inspected the employee handbook and code of conduct acknowledgement template to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct which required adherence to the personnel’s job role and responsibilities.	Testing of the control activity disclosed that no new employees were hired during the review period.
		Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.	Inspected the employee performance evaluation document to determine that policies and procedures were in place that outlined the performance evaluation process as well as the competency and training requirements for personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
		Sanction policies, which include probation, suspension, and termination, are in place for employee misconduct.	Inspected the code of conduct policies and procedures to determine that sanction policies, which include probation, suspension, and termination, were in place for employee misconduct.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's shared drive site.	Inspected the information security policies and procedures, a sample of job descriptions and the entity's shared drive to determine that organizational and information security policies and procedures were documented for supporting the functioning of controls and processes and made available to its personnel through the entity's shared drive site.	No exceptions noted.
		Data flow diagrams are documented and maintained by management to identify the relevant internal and external information sources of the system.	Inspected the data flow diagrams to determine that data flow diagrams were documented and maintained by management to identify the relevant internal and external information sources of the system.	No exceptions noted.
		Data is only retained for as long as required to perform the required system functionality, service, or use.	Inspected the backup and recovery policies and procedures to determine that data was retained for only as long as required to perform the required system functionality, service, or use.	No exceptions noted.
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's shared drive site.	Inspected a sample of job descriptions and the entity's shared drive to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's shared drive site.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity's policies and procedures, code of conduct and employee handbook are made available to employees through the entity's shared drive site.	Inspected the entity's shared drive to determine that the entity's policies and procedures, code of conduct and employee handbook were made available to employees through the entity's shared drive site.	No exceptions noted.
		Upon hire, employees are required to read and acknowledge the information security policies and procedures and complete information security and awareness training.	Inspected the signed employee handbook, code of conduct acknowledgement, and security training completion certificate for a sample of new hires to determine that upon hire, employees were required to read and acknowledge the information security policies and procedures and complete information security and awareness training.	Testing of the control activity disclosed that no new employees were hired during the review period.
			Inspected the employee handbook, code of conduct acknowledgement, and security training materials to determine that upon hire, employees were required to read and acknowledge the information security policies and procedures and complete information security and awareness training.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Current employees are required to read and acknowledge the information security policies and procedures and complete information security and awareness training on an annual basis.	Inspected the security training completion certificate for a sample of currents employee to determine that current employees were required to read and acknowledge the information security policies and procedures and complete information security and awareness training on an annual basis.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.	Inquired of the Lead Developer regarding new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
			Inspected the employee handbook and code of conduct acknowledgment template to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
			Inspected the signed employee handbook and code of conduct acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	Testing of the control activity disclosed that no new employees were hired during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.	Inquired of the Lead Developer regarding new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct which required adherence to the personnel’s job role and responsibilities.	No exceptions noted.
			Inspected the employee handbook and code of conduct acknowledgement template to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct which required adherence to the personnel’s job role and responsibilities.	No exceptions noted.
			Inspected the signed employee handbook and code of conduct acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct which required adherence to the personnel’s job role and responsibilities.	Testing of the control activity disclosed that no new employees were hired during the review period.
		An anonymous hotline is in place to allow employees, third-parties and customers to report unethical behavior in a confidential manner.	Inspected the anonymous hotline to determine that an anonymous hotline was in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the executed subscription agreement for a sample of third-parties to determine that the entity’s third-party agreement delineated the boundaries of the system and described relevant system components.	No exceptions noted.
		The entity's third-party agreement communicates the system commitments and requirements of third-parties.	Inquired of the Lead Developer, regarding third-party agreements, to determine that the entity’s third-party agreement communicated the system commitments and requirements of third-parties.	No exceptions noted.
			Inspected the subscription agreement to determine that the entity’s third-party agreement communicated the system commitments and requirements of third-parties.	No exceptions noted.
			Inspected the executed master services agreement for a sample of new clients to determine that the entity’s third-party agreement communicated the system commitments and requirements of third-parties.	Testing of this control activity disclosed that no new third-parties and clients had been acquired in the six months preceding the review date.
		Customer commitments, requirements and responsibilities are outlined and communicated through service agreements.	Inquired of the Lead Developer, regarding third-party agreements, to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the master agreement template to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.	No exceptions noted.
			Inspected the subscription agreement for a sample of new clients to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.	Testing of this control activity disclosed that no new third-parties and clients had been acquired in the six months preceding the review date.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity has defined the desired level of performance and operation in order to achieve the established entity objectives.	Inspected the key performance indicators for operational and internal controls effectiveness to determine that the entity defined the desired level of performance and operation in order to achieve the established entity objectives.	No exceptions noted.
		Executive management reviews operational and resourcing reports to evaluate performance and resourcing annually.	Inspected the annual meeting minutes to determine that executive management reviewed operational and resourcing reports to evaluate performance and resourcing annually.	No exceptions noted.
		Business plans and budgets align with the entity's strategies and objectives.	Inspected the entity's business plans, budget, and documented objectives and strategies to determine that business plans and budgets aligned with the entity's strategies and objectives.	No exceptions noted.
		The entity's internal controls framework is based on a recognized framework.	Inspected the completed attestation report to determine that the entity's internal controls framework was based on a recognized framework.	No exceptions noted.
		The entity's internal controls environment takes into consideration affecting laws, regulations, standards, and legislatures.	Inspected the internal controls matrix 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**
		The entity undergoes compliance audits annually to show compliance to relevant laws, regulations, and standards.	Inspected the entity's SOC 2 compliance report to determine that the entity underwent compliance audits annually to show compliance to relevant laws, regulations, and standards.	No exceptions noted.
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Documented policies and procedures are in place to guide personnel when performing a risk assessment.	Inspected the risk assessment policy to determine that documented policies and procedures were in place to guide personnel when performing a risk assessment.	No exceptions noted.
		Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating, and addressing risks and defining specified risk tolerances.	Inspected the risk assessment policy to determine that management defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating, and addressing risks and defining specified risk tolerances.	No exceptions noted.
		A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.
		Identified risks are rated using a risk evaluation process and ratings are approved by management.	Inspected the risk assessment policy and the completed risk assessment to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Risks identified as a part of the risk assessment process are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the risk assessment policy 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: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted. No exceptions noted.
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the risk assessment policy 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.
		For gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, are assigned to process owners based on roles and responsibilities.	Inspected the risk assessment policy and the completed risk assessment to determine that for gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, were assigned to process owners based on roles and responsibilities.	No exceptions noted.
		The annual comprehensive risk assessment results are reviewed and approved by appropriate levels of management.	Inspected the risk assessment policy and the completed risk assessment to determine that the annual comprehensive risk assessment results were reviewed and approved by appropriate levels of management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		As part of the annual risk assessment, management reviews the potential threats and vulnerabilities arising from its customers, vendors and third-parties.	Inspected the risk assessment policy and the completed risk assessment to determine that as part of the annual risk assessment, management reviewed the potential threats and vulnerabilities arising from its customers, vendors and third-parties.	No exceptions noted.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	On an annual basis, management identifies and assesses the types of fraud (e.g., fraudulent reporting, loss of assets, unauthorized system access, overriding controls) that could impact their business and operations.	Inspected the completed risk assessment to determine that, on an annual basis, management identified and assessed the types of fraud (e.g., fraudulent reporting, loss of assets, unauthorized system access, overriding controls) that could impact their business and operations.	No exceptions noted.
		As part of management's assessment of risks, management considers key fraud factors such as incentives, pressures, opportunities for unauthorized access or use of data, and employee morale and attitude.	Inspected the completed risk assessment to determine that as part of management's assessment of fraud risks, management considered key fraud factors such as incentives, pressures, opportunities for unauthorized access or use of data, and employee morale and attitude.	No exceptions noted.
		As part of management's assessment of risks, management considers how personnel could engage in or justify fraudulent activities.	Inspected the completed risk assessment to determine that as part of management's assessment of fraud risks, management considered how personnel could engage in or justify fraudulent activities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		As part of management's assessment of risks, management considers threats and vulnerabilities that arise from the use of IT (e.g., unauthorized access, inadequate segregation of duties, default accounts, inadequate password management, unauthorized changes).	Inspected the completed 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 (e.g., unauthorized access, inadequate segregation of duties, default accounts, inadequate password management, unauthorized changes).	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 policy and the completed risk assessment to determine that changes to the regulatory, economic, and physical environment in which the entity operates were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
		Changes to the business structure and operations are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the risk assessment policy and the completed risk assessment to determine that changes to the business structure and operations were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
		Changes in key management and personnel are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the risk assessment policy and the completed risk assessment to determine that changes in key management and personnel were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, intrusion detection system (IDS) configurations, and firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		On an annual basis, management reviews the controls implemented within the environment for operational effectiveness and identifies potential control gaps and weaknesses.	Inspected the annual meeting minutes for internal control effectiveness to determine that on an annual basis, management reviewed the controls implemented within the environment for operational effectiveness and identified potential control gaps and weaknesses.	No exceptions noted.
		Vulnerability scans are performed monthly on the environment to identify control gaps and vulnerabilities.	Inspected the completed vulnerability scan results for a sample of months to determine that vulnerability scans were performed monthly on the environment to identify control gaps and vulnerabilities.	No exceptions noted.

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.	A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.
		Vulnerabilities, deviations, and control gaps identified from the risk assessment are communicated to those parties responsible for taking corrective actions.	Inspected the completed risk assessment to determine that vulnerabilities, deviations, and control gaps identified from the risk assessment were communicated to those parties responsible for taking corrective actions.	No exceptions noted.
		Vulnerabilities, deviations, and control gaps identified from the risk assessment are documented, investigated, and addressed.	Inspected the completed risk assessment to determine that vulnerabilities, deviations, and control gaps identified from the risk assessment were documented, investigated, and addressed.	No exceptions noted.
		Vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments are addressed by those parties responsible for taking corrective actions.	Inspected the completed risk assessment to determine that vulnerabilities, deviations, and control gaps identified from the risk and compliance assessments were addressed by those parties responsible for taking corrective actions.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	As part of the risk assessment process, controls within the environment are modified and implemented to mitigate identified vulnerabilities, deviations, and control gaps.	Inspected the completed risk assessment to determine that as part of the risk assessment process, controls within the environment were modified and implemented to mitigate identified vulnerabilities, deviations, and control gaps.	No exceptions noted.
		Controls within the environment are modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed.	Inspected the completed risk assessment to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed.	No exceptions noted.
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Inspected the organizational chart and internal controls matrix to determine that performance of the internal controls implemented within the environment were assigned to appropriate process owners and operational personnel based on roles and responsibilities.	No exceptions noted.
		Management has documented the relevant controls in place for each key business or operational process.	Inspected the internal controls matrix to determine that management documented the relevant controls in place for each key business or operational process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	Inspected the internal controls matrix to determine that management incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	No exceptions noted.
		Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	Inspected the risk assessment policies and procedures to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
			Inspected the completed risk assessment to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
		The disaster recovery plan is tested on an annual basis.	Inspected the completed disaster recovery test results to determine that the disaster recovery plan was tested on an annual basis.	No exceptions noted.
		The business continuity and disaster recovery plan and procedures are updated based on disaster recovery plan test results.	Inspected the business continuity and disaster recovery plans and completed disaster recovery test results to determine that the business continuity and disaster recovery plan and procedures were updated based on disaster recovery plan test results.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
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 has documented the relationship and linkage between business processes, the relevant technologies used to support the business processes, and the controls in place to help secure those business processes.	Inspected the internal controls matrix to determine that management documented the relationship and linkage between business processes, the relevant technologies used to support the business processes, and the controls in place to help secure those business processes.	No exceptions noted.
		Organizational and information security policies and procedures are documented and made available to employees through the entity's shared Drive.	Inspected the information security policies and procedures to determine that organizational and information security policies and procedures were documented and made available to its personnel through the entity's shared Drive.	No exceptions noted.
		Management has documented the controls implemented around the entity's technology infrastructure.	Inspected the internal controls matrix to determine that management documented the controls implemented around the entity's technology infrastructure.	No exceptions noted.
		Management has established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.	Inspected the internal controls matrix to determine that management established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.	No exceptions noted.
		As part of the risk assessment process, the use of technology in business processes is evaluated by management.	Inspected the completed risk assessment to determine that as part of the risk assessment process, the use of technology in business processes was evaluated by management.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management has implemented controls that are built into the organizational and information security policies and procedures.	Inspected the organizational and information security policies and procedures and internal controls matrix to determine that management implemented controls that were built into the organizational and information security policies and procedures.	No exceptions noted.
		Process owners and key management are assigned ownership to each key internal control implemented within the entity's environment.	Inspected the internal controls matrix to determine that process owners and key management were assigned ownership to each key internal control implemented within the entity's environment.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's shared drive.	Inspected a sample of job descriptions to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's shared drive.	No exceptions noted.
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Inspected the internal controls matrix to determine that performance of the internal controls implemented within the environment were assigned to appropriate process owners and operational personnel based on roles and responsibilities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Process owners and management operate the controls implemented within the entity's environment based on the frequency defined in the organizational and information security policies and procedures.	Inspected the organizational and information security policies and procedures and internal controls matrix to determine that process owners and management operated the controls implemented within the entity's environment based on the frequency defined in the organizational and information security policies and procedures.	No exceptions noted.
		Process owners and management investigate and troubleshoot control failures.	Inspected the completed risk assessment to determine that process owners and management investigated and troubleshot control failures.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	An inventory of system assets and components is maintained to classify and manage the information assets.	Inspected the inventory listing of system assets and components to determine that the inventory of system assets and components was maintained to classify and manage the information assets.	No exceptions noted.
		Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the Lead Developer, regarding access to sensitive resources, to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
			Inspected the listings of privileged users to the network, database, and application to determine that privileged access to sensitive resources was restricted to authorized personnel.	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.
	Network			
		Network user access is restricted via role-based security privileges defined within the access control system.	Inspected the network user listing and access rights to determine that network user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Logical and Physical Access Controls

CC6.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Network administrative access is restricted to the appropriate personnel.	Inquired of the Lead Developer, regarding network administrators, to determine that network administrative access was restricted to authorized personnel.	No exceptions noted.
			Inspected the network administrator listing to determine that network administrative access was restricted to the appropriate personnel.	No exceptions noted.
		Network users are authenticated via individually assigned user accounts and passwords. Networks are configured to enforce password requirements that include: • Password length • Password history • Complexity	Inspected the network authentication settings to determine that network users were authenticated via individually assigned user accounts and passwords. Networks were configured to enforce password requirements that include: • Password length • Password history • Complexity	No exceptions noted.

<table>
<tr><th colspan="5">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="5">Logical and Physical Access Controls</th></tr>
<tr><th>CC6.0</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td></td><td></td><td>Network audit policy configurations are in place that include:
• Account logon events
• Account management
• Directory Service Access
• Logon events
• Object access
• Policy changes
• Privilege use
• Process tracking
• System events</td><td>Inspected the network audit logging policy and a sample of network log extracts to determine that network audit policy configurations were in place that include:
• Account logon events
• Account management
• Directory Service Access
• Logon events
• Object access
• Policy changes
• Privilege use
• Process tracking
• System events</td><td>No exceptions noted.</td></tr>
<tr><td></td><td colspan="4"><b>Database</b></td></tr>
<tr><td></td><td></td><td>Database user access is restricted via role-based security privileges defined within the access control system.</td><td>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.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>Database administrative access is restricted to the appropriate personnel.</td><td>Inquired of the Lead Developer, regarding database administrators, to determine that database administrative access was restricted to authorized personnel.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td></td><td>Inspected the database administrator listing to determine that database administrative access was restricted to authorized personnel.</td><td>No exceptions noted.</td></tr>
</table>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Database users are authenticated via individually assigned user accounts and passwords. Databases are configured to enforce password requirements that include: • Password length • Password history • Password age • Complexity	Inspected the database authentication settings to determine that database users were authenticated via individually assigned user accounts and passwords. Databases were configured to enforce password requirements that include: • Password length • Password history • Password age • Complexity	No exceptions noted.
		Database audit policy configurations are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the database audit logging policy and a sample of database log extracts to determine that database audit policy configurations were in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.
	Application			
		Application user access is restricted via role-based security privileges defined within the access control system.	Inspected the application user listing and access rights to determine that application user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

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 administrative access is restricted to the appropriate personnel.	Inquired of the Lead Developer, regarding application administrators, to determine that application administrative access was restricted to authorized personnel.	No exceptions noted.
			Inspected the application administrator listing to determine that application administrative access was restricted to authorized personnel.	No exceptions noted.
		Application users are authenticated via individually assigned user accounts and passwords. Applications are configured to enforce password requirements that include: • Password length • Complexity	Inspected the application authentication settings to determine that application users were authenticated via individually assigned user accounts and passwords. Applications were configured to enforce password requirements that include: • Password length • Complexity	No exceptions noted.
		Application account lockout settings are in place that include: • Account lockout threshold • Account lockout duration • Account lockout counter reset	Inspected account lockout settings to determine that application account lockout settings were in place that include: • Account lockout threshold • Account lockout duration • Account lockout counter reset	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Application audit policy configurations are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the application audit logging policy and a sample of application log extracts to determine that application audit policy configurations were in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.
		Data coming into the environment is secured and monitored using firewalls and an IDS (Intrusion Detection System).	Inspected the IDS configurations, firewall rule sets, and the network diagram to determine that data coming into the environment was secured and monitored using firewalls and an IDS.	No exceptions noted.
		Critical data is stored in encrypted format using software supporting the AES (Advanced Encryption Standard) encryption.	Inspected the encryption configurations for data at rest to determine that critical data was stored in encrypted format using AES encryption.	No exceptions noted.
		Control self-assessments that include physical and logical access reviews are performed on an annual basis.	Inspected the completed network user access review, database user access review, and application user access review to determine that control self-assessments that included physical and logical access reviews were performed on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Logical access to systems is granted to an employee as a component of the hiring process.	Inquired of the Lead Developer regarding logical access to system to determine that logical and physical access to systems was granted to an employee as a component of the hiring process.	No exceptions noted.
			Inspected the information security policy to determine that logical and physical access to systems was granted to an employee as a component of the hiring process.	No exceptions noted.
			Inspected the access request ticket for a sample of new hires to determine that logical and physical access to systems was granted to an employee as a component of the hiring process.	Testing of the control activity disclosed that no new employees were hired during the review period.
		Logical access to systems is revoked as a component of the termination process.	Inquired of the Lead Developer, regarding terminated employees, to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.
			Inspected the information security policy to determine that logical and physical access to systems was revoked to an employee as a component of the termination process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the termination procedures, network, operating system, database, application, and user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked for an employee as a component of the termination process.	Testing of the control activity disclosed that no employees were terminated during the review period.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
		Logical access to systems is granted to an employee as a component of the hiring process.	Inquired of the Lead Developer regarding logical access to system to determine that logical and physical access to systems was granted to an employee as a component of the hiring process.	No exceptions noted.
			Inspected the information security policy to determine that logical and physical access to systems was granted to an employee as a component of the hiring process.	No exceptions noted.
			Inspected the access request ticket for a sample of new hires to determine that logical and physical access to systems was granted to an employee as a component of the hiring process.	Testing of the control activity disclosed that no new employees were hired during the review period.

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 Lead Developer, regarding terminated employees, to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.
			Inspected the information security policy to determine that logical and physical access to systems was revoked to an employee as a component of the termination process.	No exceptions noted.
			Inspected the termination procedures, network, operating system, database, application, and user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked for an employee as a component of the termination process.	Testing of the control activity disclosed that no employees were terminated during the review period.
		Control self-assessments that include physical and logical access reviews are performed on an annual basis.	Inspected the completed network user access review, database user access review, and application user access review to determine that control self-assessments that included physical and logical access reviews were performed on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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, considering the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the Lead Developer, regarding access to sensitive resources, to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
			Inspected the listings of privileged users to the network, database, and application to determine that privileged access to sensitive resources was restricted to authorized personnel.	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 granted to an employee as a component of the hiring process.	Inquired of the Lead Developer regarding logical access to system to determine that logical and physical access to systems was granted to an employee as a component of the hiring process.	No exceptions noted.
			Inspected the information security policy, and the hiring and recruiting policy to determine that logical and physical access to systems was granted to an employee as a component of the hiring process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the access request ticket for a sample of new hires to determine that logical and physical access to systems was granted to an employee as a component of the hiring process.	Testing of the control activity disclosed that no new employees were hired during the review period.
		Logical access to systems is revoked as a component of the termination process.	Inquired of the Lead Developer, regarding terminated employees, to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.
			Inspected the information security policy to determine that logical and physical access to systems was revoked to an employee as a component of the termination process.	No exceptions noted.
			Inspected the termination procedures, network, operating system, database, application, and user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked for an employee as a component of the termination process.	Testing of the control activity disclosed that no employees were terminated during the review period.
		Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the Lead Developer, regarding access to sensitive resources, to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the listings of privileged users to the network, database, and application to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
		Control self-assessments that include physical and logical access reviews are performed on an annual basis.	Inspected the completed network user access review, database user access review, and application user access review to determine that control self-assessments that included physical and logical access reviews were performed on an annual basis.	No exceptions noted.
	Network			
		Network access reviews are completed by management on an annual basis.	Inspected the completed network access review to determine that network access reviews were completed by management on an annual basis.	No exceptions noted.
		Network user access is restricted via role-based security privileges defined within the access control system.	Inspected the network user listing and access rights to determine that network user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
	Database			
		Database access reviews are completed by management on an annual basis.	Inspected the completed database access review to determine that database access reviews were completed by management on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Database user access is restricted via role-based security privileges defined within the access control system.	Inspected the database user listing and access rights to determine that database user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
	Application			
		Application access reviews are completed by management on an annual basis.	Inspected the completed application access review to determine that application access reviews were completed by management on an annual basis.	No exceptions noted.
		Application user access is restricted via role-based security privileges defined within the access control system.	Inspected the application user listing and access rights to determine that application user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	This criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
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 policy to determine that 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**
		Policies and procedures are in place for removal of media storing critical data or software.	Inspected the data disposal policy to determine that policies and procedures were in place for removal of media storing critical data or software.	No exceptions noted.
		The entity purges data stored on backup tapes and backup drives, per a defined schedule.	Inspected the data disposal policy to determine that the entity purged data stored on backup tapes and backup drives, per a defined schedule.	No exceptions noted.
		Data that is no longer required for business purposes is rendered unreadable.	Inquired of the Lead Developer, regarding data disposal practices, to determine that data that was no longer required for business purposes was rendered unreadable and no longer accessible within the system.	No exceptions noted.
			Inspected the data disposal policy to determine that data that was no longer required for business purposes was rendered unreadable.	No exceptions noted.
			Inspected the completed service ticket for a sample of requests to dispose of data, purge a system, or physically destroy a system, to determine that data that was no longer required for business purposes was rendered unreadable.	Testing of the control activity disclosed that there were no requests to dispose of data, during the review period.

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.	Server certificate-based authentication is used as part of the SSL encryption with a trusted certificate authority.	Inspected the encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the SSL encryption with a trusted certificate authority.	No exceptions noted.
		Transmission of digital output beyond the boundary of the system is encrypted.	Inspected the encryption configurations for data in transit and digital certificates to determine that transmission of digital output beyond the boundary of the system was encrypted.	No exceptions noted.
		Logical access to stored data is restricted to authorized personnel.	Inquired of the Lead Developer, regarding access to stored data, to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
			Inspected the network, database, and application user listings and access rights to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
			Inspected the firewall rule sets for the production servers to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.

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

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

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

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**
		An IDS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected the IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS is configured to notify personnel upon intrusion detection.	Inspected an IDS alert notification to determine that the IDS was configured to notify personnel upon intrusion detection.	No exceptions noted.
		Critical data is stored in encrypted format using software supporting the AES encryption.	Inspected the encryption configurations for data at rest to determine that critical data was stored in encrypted format using AES encryption.	No exceptions noted.
		Backup media is stored in an encrypted format.	Inspected the encryption configurations to determine that backup media was stored in an encrypted format.	No exceptions noted.
		Transmission of digital output beyond the boundary of the system is encrypted.	Inspected the encryption configurations for data in transit and digital certificates to determine that transmission of digital output beyond the boundary of the system was encrypted.	No exceptions noted.
		Policies and procedures are in place for removal of media storing critical data or software.	Inspected the data disposal policy to determine that policies and procedures were in place for removal of media storing critical data or software.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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.	The ability to migrate changes into the production environment is restricted to authorized and appropriate users.	Inquired of the Lead Developer, regarding production access, to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users.	No exceptions noted.
			Inspected the list of users with the ability to implement changes into the production environment to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users.	No exceptions noted.
		Segregation of duties in the change management policy are utilized to ensure only authorized changes are deployed into the production environment.	Inspected the information security policies and procedures to determine that segregation of duties was utilized to ensure only authorized changes are deployed into the production environment.	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.
		Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus software dashboard console to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		The antivirus software provider pushes updates in real-time to the installed antivirus software as current updates /signatures are available.	Inspected the antivirus settings to determine that the antivirus software provider pushed updates in real-time to the installed antivirus software as current updates/signatures were available.	No exceptions noted.
		The antivirus software is configured to scan workstations on a weekly basis.	Inspected the antivirus settings to determine that the antivirus software was configured to scan workstations on a weekly basis.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		The IDS is configured to notify personnel upon intrusion detection.	Inspected an IDS alert notification to determine that the IDS was configured to notify personnel upon intrusion detection.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the removable media policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
			Inspected the firewall rule sets for the production servers to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
			Inspected the firewall rule sets for the production servers to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

System Operations

CC7.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity’s ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected the information security and incident management policies and procedures to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	No exceptions noted.
		Vulnerability scans are performed monthly on the environment to identify control gaps and vulnerabilities.	Inspected the completed vulnerability scan results for a sample of months to determine that vulnerability scans were performed monthly on the environment to identify control gaps and vulnerabilities.	No exceptions noted.
		Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident response policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected the information security and incident policies and procedures to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations, the antivirus software dashboard console, IDS configurations, and firewall rule sets to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.
		Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, IDS configurations, and firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		An IDS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected the IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS is configured to notify personnel upon intrusion detection.	Inspected an IDS alert notification to determine that the IDS was configured to notify personnel upon intrusion detection.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus software dashboard console to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
		The antivirus software provider pushes updates in real time to the installed antivirus software as new updates/signatures are available.	Inspected the antivirus settings to determine that the antivirus software provider pushed updates in real time to the installed antivirus software as new updates/signatures were available.	No exceptions noted.
		The antivirus software is configured to scan workstations on a weekly basis.	Inspected the antivirus settings to determine that the antivirus software was configured to scan workstations on a weekly basis.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the information security policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Network			
		Network audit logging settings are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the network audit logging settings to determine that network audit logging configurations were in place that included: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.
		Network audit logs are maintained and reviewed annually.	Inspected a network log extract to determine that network audit logs were maintained and reviewed annually.	No exceptions noted.
	Database			
		Database audit logging settings are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the database audit logging settings to determine that database audit logging configurations were in place that included: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Database audit logs are maintained and reviewed annually.	Inspected a database log extract to determine that database audit logs were maintained and reviewed annually.	No exceptions noted.
	Application			
		Application audit logging settings are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the application audit logging settings to determine that application audit logging configurations were in place that included: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.
		Application audit logs are maintained and reviewed annually.	Inspected an application log extract to determine that application audit logs were maintained and reviewed annually.	No exceptions noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident response policies and procedures and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The incident response policies and procedures define the classification of incidents based on its severity.	Inspected the incident response policies and procedures to determine that the incident response policies and procedures defined the classification of incidents based on its severity.	No exceptions noted.
		Resolution of incidents are documented within the ticket and communicated to affected users.	Inquired of the Lead Developer, regarding security incident procedures, to determine that resolution of incidents was documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that the resolution of incidents was documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that resolution of incidents was documented within the ticket and communicated to affected users.	Testing of the control activity disclosed that there were no incidents during the review period.
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inquired of the Lead Developer, regarding security incident procedures to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.

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

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

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Critical security incidents that result in a service/business operation disruption are communicated to those affected through creation of an incident ticket.	Inquired of the Lead Developer, regarding critical security incidents, to determine that critical security incidents that result in a service/business operation disruption were communicated to those affected through creation of an incident ticket.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that critical security incidents that result in a service/business operation disruption were communicated to those affected through creation of an incident ticket.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of critical security incidents that resulted in a service/business operation disruption to determine that critical security incidents that result in a service/business operation disruption were communicated to those affected.	Testing of the control activity disclosed that there were no critical security incidents during the review period.
		Resolution of incidents are documented within the ticket and communicated to affected users.	Inquired of the Lead Developer, regarding security incident procedures, to determine that resolution of incidents was documented within the ticket and communicated to affected users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the incident response policies and procedures to determine that resolution of incidents was documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the correlating ticket for a sample of incidents to determine that resolution of incidents was documented within the ticket and communicated to affected users.	Testing of the control activity disclosed that there were no incidents during the review period.
		Remediation actions taken for security incidents are documented within the ticket and communicated to affected users.	Inquired of the Lead Developer, regarding security incident procedures, to determine that the remediation actions taken for security incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that the remediation actions taken for security incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the correlating ticket for a sample of incidents to determine that the remediation actions taken for security incidents were documented within the ticket and communicated to affected users.	Testing of the control activity disclosed that there were no critical security incidents during the review period.

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

<table>
<tr><th colspan="5">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="5">System Operations</th></tr>
<tr><th>CC7.0</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td>CC7.5</td><td>The entity identifies, develops, and implements activities to recover from identified security incidents.</td><td>Change management requests are opened for incidents that require permanent fixes.</td><td>Inspected the change management policies and procedures to determine that change management requests were required to be opened for incidents that required permanent fixes.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>The entity restores system operations for incidents impacting the environment through activities that include, but are not limited to: rebuilding systems
• Rebuilding systems
• Updating software
• Installing patches
• Removing unauthorized access
• Changing configurations</td><td>Inspected the information security, incident, and change management policies and procedures, to determine that the entity restored system operations for incidents impacting the environment through activities that included, but were not limited to:
• Rebuilding systems
• Updating software
• Installing patches
• Removing unauthorized access
• Changing configurations</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>Data backup and restore procedures are in place to guide personnel in performing backup activities.</td><td>Inspected the backup policies and procedures to determine that data backup and restore procedures were in place to guide personnel in performing backup activities.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>A business continuity and disaster recovery plan are documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.</td><td>Inspected the business continuity and disaster recovery plans to determine that a business continuity and disaster recovery plan was documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.</td><td>No exceptions noted.</td></tr>
</table>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		The disaster recovery plan is tested on an annual basis.	Inspected the completed disaster recovery test results to determine that the disaster recovery plan was tested on an annual basis.	No exceptions noted.
		The business continuity and disaster recovery plan and procedures are updated based on disaster recovery plan test results.	Inspected the business continuity and disaster recovery plans and completed business continuity and disaster recovery test results to determine that the business continuity and disaster recovery plan and procedures were updated based on disaster recovery plan test results.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.1	The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Documented change control policies and procedures are in place to guide personnel in the change management process.	Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in the change management process.	No exceptions noted.
		The change management process has defined the following roles and assignments: • Authorization of change requests-owner or business unit manager • Development-application design and support department • Testing-quality assurance department • Implementation software change management group	Inspected the change management policies and procedures to determine that the change management process defined the following roles and assignments: • Authorization of change requests-owner or business unit manager • Development-application design and support department • Testing-quality assurance department • Implementation software change management group	No exceptions noted.
		System changes are communicated to both affected internal and external users.	Inspected the correlating change ticket for a sample of system changes to determine that system changes were communicated to both affected internal and external users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Access to implement changes in the production environment is restricted to authorized personnel.	Inspected the list of users with access to deploy changes into the production environment to determine that access to implement changes in the production environment was restricted to authorized personnel.	No exceptions noted.
		System changes are authorized and approved by management prior to implementation.	Inspected the correlating change ticket for a sample of system changes, and a sample of code changes to determine that system changes were authorized and approved by management prior to implementation.	No exceptions noted.
		System change requests are documented and tracked in a ticketing system.	Inspected the correlating change ticket a sample of system changes to determine that system change requests were documented and tracked in a ticketing system.	No exceptions noted.
		System changes are tested prior to implementation when required and types of testing performed depend on the nature of the change.	Inspected the change management policies and procedures to determine that system changes were tested prior to implementation when required and types of testing performed depended on the nature of the change.	No exceptions noted.
			Inspected the correlating change ticket for a sample of system changes to determine that system changes were tested prior to implementation and types of testing performed depended on the nature of the change.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency.	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.	No exceptions noted.

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

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management develops third-party risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the vendor management policies and procedures and the completed vendor risk assessment to determine that management developed third-party risk mitigation strategies to address risks identified during the third-party risk assessment process.	No exceptions noted.
		Identified third-party risks are rated using a risk evaluation process and ratings are approved by management.	Inspected the vendor management policies and procedures and the completed vendor risk assessment to determine that identified third-party risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
		The entity's third-party agreement outlines and communicates the terms, conditions, and responsibilities of third-parties.	Inquired of the Lead Developer, regarding subscription agreements, to determine that the entity's third-party agreement outlined and communicated the terms, conditions, and responsibilities of third-parties.	No exceptions noted.
			Inspected the subscription agreement template to determine that the entity's third-party agreement outlined and communicated the terms, conditions, and responsibilities of third-parties.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the executed subscription agreement for a sample of clients to determine that the entity's third-party agreement outlined and communicated the terms, conditions, and responsibilities of third-parties.	Testing of this control activity disclosed that no new third-parties and clients had been acquired during the review period.
		Management obtains and reviews attestation reports of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Inspected the completed vendor risk assessment and attestation report for a sample of third-parties to determine that management obtained and reviewed attestation reports of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	No exceptions noted.
		A formal third-party risk assessment is performed on an annual basis to identify threats that could impair system commitments and requirements.	Inspected the vendor management policies and procedures to determine that a formal third-party risk assessment was performed on an annual basis to identify threats that could impair system commitments and requirements.	No exceptions noted.
		Management has established exception handling procedures for services provided by third-parties.	Inspected the vendor management policies and procedures to determine that management established exception handling procedures for services provided by third-parties.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		The entity has documented procedures for addressing issues identified with third-parties.	Inspected the vendor management policies and procedures to determine that the entity documented procedures for addressing issues identified with third-parties.	No exceptions noted.
		The entity has documented procedures for terminating third-party relationships.	Inspected the vendor management policies and procedures to determine that the entity documented procedures for terminating third-party relationships.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE CONFIDENTIALITY CATEGORY				
C1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Documented confidential policies and procedures are in place that include the following: • Defining, identifying, and designating information as confidential • Storing confidential information • Protecting confidential information from erasure or destruction • Retaining confidential information for only if is required to achieve the purpose for which the data was collected and processed	Inspected the confidentiality policies and procedures to determine that documented confidential policies and procedures were in place that included: • Defining, identifying, and designating information as confidential • Storing confidential information • Protecting confidential information from erasure or destruction • Retaining confidential information for only if is required to achieve the purpose for which the data was collected and processed	No exceptions noted.
		An inventory log is maintained of assets with confidential data.	Inspected the master list of system components to determine that an inventory log was maintained of assets with confidential data.	No exceptions noted.
		Confidential information is protected from erasure or destruction during the specified retention period.	Inspected the confidentiality policies and procedures to determine that confidential information was protected from erasure or destruction during the specified retention period.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE CONFIDENTIALITY CATEGORY				
C1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	Documented data destruction policies and procedures are in place that include the following: • Identifying confidential information requiring destruction when the end of the retention period is reached • Erasing or destroying confidential information that has been identified for destruction	Inspected the data destruction policies and procedures to determine that documented data destruction policies and procedures were in place that included: • Identifying confidential information requiring destruction when the end of the retention period is reached • Erasing or destroying confidential information that has been identified for destruction	No exceptions noted.
		An inventory log is maintained of assets with confidential data, and as confidential data meets the retention period, the data is destroyed or purged.	Inspected the master list of system components to determine that an inventory log was maintained of assets with confidential data, and as confidential data met the retention period, the data was destroyed or purged.	No exceptions noted.
		The entity purges confidential data after it is no longer required to achieve the purpose for which the data was collected and processed.	Inquired of the Lead Developer, regarding disposal of confidential data, to determine that the entity purged confidential data after it was no longer required to achieve the purpose for which the data was collected and processed.	No exceptions noted.
			Inspected the data destruction policies and procedures to determine that the entity purged confidential data after it was no longer required to achieve the purpose for which the data was collected and processed.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE CONFIDENTIALITY CATEGORY				
C1.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the correlating tickets for a sample of requests to purge data or destroy a system to determine that the entity purged confidential data after it was no longer required to achieve the purpose for which the data was collected and processed.	Testing of this control activity disclosed that no requests to purge data or destroy a system occurred in the six months preceding the review date.