A-LIGN

3rd Millennium Classrooms

Type 2 SOC 2

2024

REPORT ON 3RD MILLENNIUM CLASSROOMS' DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS RELEVANT TO SECURITY

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

December 1, 2023 to November 30, 2024

Table of Contents

SECTION 1

ASSERTION OF 3RD MILLENNIUM CLASSROOMS MANAGEMENT

ASSERTION OF 3RD MILLENNIUM CLASSROOMS MANAGEMENT

December 6, 2024

We have prepared the accompanying description of 3rd Millennium Classrooms' ('3rd Millennium' or 'the Company') E-Learning Program Services System titled "3rd Millennium Classrooms' Description of Its E-Learning Program Services System throughout the period December 1, 2023 to November 30, 2024" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the E-Learning Program Services System that may be useful when assessing the risks arising from interactions with 3rd Millennium's system, particularly information about system controls that 3rd Millennium has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

3rd Millennium uses DigitalOcean Holdings, Inc. ('DigitalOcean' 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 3rd Millennium, to achieve 3rd Millennium's service commitments and system requirements based on the applicable trust services criteria. The description presents 3rd Millennium's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of 3rd Millennium'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 3rd Millennium, to achieve 3rd Millennium's service commitments and system requirements based on the applicable trust services criteria. The description presents 3rd Millennium's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of 3rd Millennium's controls.

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

a. the description presents 3rd Millennium's E-Learning Program Services System that was designed and implemented throughout the period December 1, 2023 to November 30, 2024, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period December 1, 2023 to November 30, 2024, to provide reasonable assurance that 3rd Millennium'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 3rd Millennium's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period December 1, 2023 to November 30, 2024, to provide reasonable assurance that 3rd Millennium'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 3rd Millennium's controls operated effectively throughout that period.

Katie McCall
Chief Executive Officer
3rd Millennium Classrooms

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: 3rd Millennium Classrooms

Scope

We have examined 3rd Millennium's accompanying description of its E-Learning Program Services System titled "3rd Millennium Classrooms' Description of Its E-Learning Program Services System throughout the period December 1, 2023 to November 30, 2024" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period December 1, 2023 to November 30, 2024, to provide reasonable assurance that 3rd Millennium's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

3rd Millennium uses DigitalOcean 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 3rd Millennium, to achieve 3rd Millennium's service commitments and system requirements based on the applicable trust services criteria. The description presents 3rd Millennium's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of 3rd Millennium'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 3rd Millennium, to achieve 3rd Millennium's service commitments and system requirements based on the applicable trust services criteria. The description presents 3rd Millennium's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of 3rd Millennium'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

3rd Millennium 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 3rd Millennium's service commitments and system requirements were achieved. 3rd Millennium has provided the accompanying assertion titled "Assertion of 3rd Millennium Classrooms Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. 3rd Millennium 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 3rd Millennium's E-Learning Program Services System that was designed and implemented throughout the period December 1, 2023 to November 30, 2024, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period December 1, 2023 to November 30, 2024, to provide reasonable assurance that 3rd Millennium'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 3rd Millennium's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period December 1, 2023 to November 30, 2024, to provide reasonable assurance that 3rd Millennium'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 3rd Millennium'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 3rd Millennium, user entities of 3rd Millennium's E-Learning Program Services System during some or all of the period December 1, 2023 to November 30, 2024, business partners of 3rd Millennium subject to risks arising from interactions with the E-Learning Program Services System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

A-LIGN ASSURANCE

Tampa, Florida
December 6, 2024

SECTION 3

3RD MILLENNIUM CLASSROOMS' DESCRIPTION OF ITS E-LEARNING PROGRAM SERVICES SYSTEM THROUGHOUT THE PERIOD DECEMBER 1, 2023 TO NOVEMBER 30, 2024

OVERVIEW OF OPERATIONS

Company Background

3rd Millennium has been at the forefront of prevention and intervention since 1999 after creating and developing the first online alcohol education course in the country. Since then, 3rd Millennium has developed courses for cannabis and other drug use, intimate partner violence and sexual consent, nicotine awareness, theft and impulse control, academic integrity, and mental health and wellness.

All of 3rd Millennium's programs use a motivational interviewing style and provide personalized feedback reports. 3rd Millennium's goal is to engage the student in a powerful learning experience that impacts behavior.

Description of Services Provided

3rd Millennium provides online behavior changes courses for use by colleges, high schools, courts, and individuals. Courses cover topics like alcohol, cannabis, nicotine, prescription and illicit drug use, shoplifting, theft and impulse control, hazing, anger management, conflict resolution, intimate partner violence and sexual consent, human trafficking, academic integrity, and mental health and wellness.

Principal Service Commitments and System Requirements

3rd Millennium designs its processes and procedures related to its E-Learning Program Services to meet its objectives for its online classroom services. Those objectives are based on the service commitments that 3rd Millennium makes to user entities, the laws and regulations that govern the provision of online classroom services, and the financial, operational, and compliance requirements that 3rd Millennium has established for the services. The online classroom services of 3rd Millennium are subject to the security and privacy requirements of the Health Insurance Portability and Accountability Act Administrative Simplification, as amended, including relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which 3rd Millennium operates.

Security commitments to user entities are documented and communicated within the privacy policy on the 3rd Millennium website, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

Security principles within the fundamental designs of the E-Learning Program 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.

3rd Millennium establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in 3rd Millennium's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the E-Learning Program Services.

Components of the System

Infrastructure

Primary infrastructure used to provide 3rd Millennium's E-Learning Program Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Web Servers	s-4vcpu-8gb, g-16vcpu-64gb, s-8vcpu-16gb, s-4vcpu-16gb-320gb-intel, s-2vcpu-8gb-160gb-intel, s-1vcpu-1gb, s-1vcpu-1gb, s-1vcpu-512mb-10gb, s-8vcpu-16gb, s-4vcpu-8gb, s-4vcpu-8gb	Host files to support the web applications
DB Clusters	2 GB RAM / 30 GB Disk / NYC3 - MySQL 8, 64 GB RAM / 1220 GB Disk / NYC3 - MySQL 8, 16 GB RAM / 290 GB Disk / NYC3 - MySQL 8	Host data
Volumes	pvc-23117a68-7196-4241-8512-d564f0d84825 (NYC3 / 10 GB), pvc-7fba070f-19ab-4a04-b07e-20d621e4bc75 (NYC3 / 25 GB), pvc-dad6e90d-2c21-49f9-ab83-67d20e02b572 (NYC3 / 10 GB)	Store data attached to containers and extension to servers

Software

Primary software used to provide 3rd Millennium's E-Learning Program Services System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
SMS	Ubuntu 22.04 (LTS) x64, Symfony 4.4, PHP 7.4.20	Provide admin control over Student Management System
Courses	Ubuntu 22.04 (LTS) x64, WordPress 6.6.2, LearnDash 4.14.0, PHP 8.0	Provide courses interface both for admin and students
Marketing	Kubernetes	Website for prospects
API	Kubernetes	API Gateway to manage all our internal micro services and data flow

People

3rd Millennium has a small in-house staff of less than 20 employees. 3rd Millennium work with dedicated contractors to provide services related to technology services and marketing.

Data

3rd Millennium uses data collected through survey questions in the course to provide personalized feedback as a part of the course experience. Aggregated student answers are provided to the administrator at the school/court upon request but are de-identified. 3rd Millennium also collects login attempts.

Processes, Policies and Procedures

Formal information technology (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 3rd Millennium policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any 3rd Millennium team member.

Physical Security

The in-scope system and supporting infrastructure is hosted by DigitalOcean. As such, DigitalOcean is responsible for the physical security controls for the in-scope system.

Logical Access

3rd Millennium uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists. In the event incompatible responsibilities cannot be segregated, 3rd Millennium implements monitoring of one or more of the responsibilities. Monitoring must be performed by a superior without responsibility for performing the conflicting activities or by personnel from a separate department.

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

Employees and approved vendor personnel sign on to the 3rd Millennium's network using Google Service and separate website login systems. Passwords must conform to defined password standards and are enforced through parameter settings. These settings are part of the configuration standards and force users to change passwords at a defined interval, disable the user ID's ability to access the system and components after a specified number of unsuccessful access attempts, and mask workstation screens, requiring reentry of the user ID and password after a period of inactivity.

Customer employees access E-Learning Program Services through the Internet using the secure socket layer (SSL) functionality of their web-browser. These customer employees must supply a valid user ID and password to gain access to customer cloud resources. Passwords must conform to password configuration requirements configured on the virtual devices using the virtual server administration account. Virtual devices are initially configured in accordance with 3rd Millennium's configuration standards, but these configuration parameters may be changed by the virtual server administration account.

Upon hire, management fills out a User Access form for the new employee. User Access Forms are updated for employees who transition to different roles within the company and need new or different systems access.

User access is granted by management, the Chief Project Officer, or by the technical team (tracked through a JIRA ticket).

On an annual basis, access rules for each role are reviewed by management and development team members. In evaluating role access, group members consider job description, duties requiring segregation, and risks associated with access.

Computer Operations - Backups

Customer data is backed up and monitored by operations personnel for completion and exceptions. In the event of an exception, operations personnel perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup.

Backups are handled through Digital Ocean. All backups are digital and stored within the Digital Ocean data centers. The ability to recall backups is restricted to authorized operations personnel.

Computer Operations - Availability

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

3rd Millennium monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches service level standards. 3rd Millennium evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Disk storage
- Network bandwidth

3rd Millennium has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Customers and E-Learning Program Services System owners review proposed operating system patches to determine whether the patches are applied. E-Learning Program Services Systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. 3rd Millennium's staff validate that all patches have been installed and if applicable that reboots have been completed.

Change Control

3rd Millennium maintains policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

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

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

3rd Millennium has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Customers and 3rd Millennium Classroom's system owners review proposed operating system patches to determine whether the patches are applied. Customers and 3rd Millennium Classroom's systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. 3rd Millennium Classroom's staff validate that all patches have been installed and if applicable that reboots have been completed.

Data Communications

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

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

Penetration testing is conducted to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology specified by 3rd Millennium. The third-party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed on a quarterly basis in accordance with 3rd Millennium policy. The third-party vendor uses industry standard scanning technologies, and a formal methodology specified by 3rd Millennium. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. Scans are performed during non-peak windows. Tools requiring installation in the E-Learning Program Services System are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Penetration testing is conducted on an annual basis to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology specified by 3rd Millennium. The third-party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network.

Boundaries of the System

The scope of this report includes the E-Learning Program Services System performed in the San Antonio, Texas facilities.

This report does not include the cloud hosting services provided by DigitalOcean at various 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 3rd Millennium's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of 3rd Millennium ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

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

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

Commitment to Competence

3rd Millennium'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

3rd Millennium'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 and its team are briefed on regulatory and industry changes affecting the services provided
- Executive management and team meetings are held on a weekly basis to discuss major initiatives and issues that affect the business as a whole

Organizational Structure and Assignment of Authority and Responsibility

3rd Millennium'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.

3rd Millennium's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

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

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

Human Resources Policies and Practices

3rd Millennium's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensure the service organization operates at maximum efficiency. 3rd Millennium'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 onboarding (first week of employment).
- Evaluations for each employee are performed on an annual basis. New employees have an initial probationary period with additional training and reviews.
- Employee termination procedures are in place to guide the termination process.

Risk Assessment Process

3rd Millennium's risk assessment process identifies and manages risks that could potentially affect 3rd Millennium Classroom's ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. 3rd Millennium identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by 3rd Millennium, and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

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

3rd Millennium has established an independent organizational business unit that is responsible for identifying risks to the entity and monitoring the operation of the firm's internal controls. The approach is intended to align the entity's strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. 3rd Millennium attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of 3rd Millennium's E-Learning Program Services System; as well as the nature of the components of the system result in risks that the criteria will not be met. 3rd Millennium 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, 3rd Millennium's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communications Systems

Information and communication are an integral component of 3rd Millennium's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At 3rd Millennium, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Weekly standup meetings are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. Senior executives lead the meetings with information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. Weekly e-mails update all staff on development activities, updates, product changes/launches, and general updates to entity-wide security policies and procedures.

Specific information systems used to support 3rd Millennium Classroom's E-Learning Program Services System are described in the Description of Services section above.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. 3rd Millennium's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

3rd Millennium'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 3rd Millennium'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 3rd Millennium's personnel.

Reporting Deficiencies

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

Changes to the System Since the Last Review

No significant changes have occurred to the services provided to user entities since 3rd Millennium's last review.

Incidents Since the Last Review

No significant incidents have occurred to the services provided to user entities since 3rd Millennium's last review.

Criteria Not Applicable to the System

All Common/Security criterion was applicable to 3rd Millennium's E-Learning Program Services System.

Subservice Organizations

This report does not include the cloud hosting services provided by DigitalOcean at various facilities.

Subservice Description of Services

DigitalOcean is responsible for the server management of the in-scope application.

Complementary Subservice Organization Controls

3rd Millennium's services are designed with the assumption that certain controls will be implemented by the subservice organization. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to 3rd Millennium's services to be solely achieved by 3rd Millennium's control procedures. Accordingly, the subservice organization, in conjunction with the services, should establish their own internal controls or procedures to complement those of 3rd Millennium.

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

Subservice Organization - DigitalOcean		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4	Documented physical security policies and procedures are in place to guide employees in the granting, controlling, and monitoring of physical access to and within the data center. Management reviews physical security policies and procedures on an annual basis.

Subservice Organization - DigitalOcean		
Category	**Criteria**	**Control**
		Physical access to data center facilities is documented and granted based on manager approval.
		Physical access is disabled within 24 business hours of notification.
		Appropriateness of physical access to data center facilities is reviewed on a semi-annual basis.
		Physical safeguards are in place to restrict access to DigitalOcean owned data centers including proximity cards, security guards, biometric scanners, alarm systems, and CCTV monitoring.

3rd Millennium's 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, 3rd Millennium Classroom's performs monitoring of the subservice organization controls, including the following procedures:

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

COMPLEMENTARY USER ENTITY CONTROLS

3rd Millennium'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 3rd Millennium's services to be solely achieved by 3rd Millennium's control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of 3rd Millennium.

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 3rd Millennium.
2. User entities are responsible for notifying 3rd Millennium 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 3rd Millennium 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 3rd Millennium's services.
6. User entities are responsible for providing 3rd Millennium with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying 3rd Millennium of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

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

Control Activities Specified by the Service Organization

The applicable trust services criteria, risks, and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing them in this section. Although the applicable trust services criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of 3rd Millennium's description of the system. Any applicable trust services criteria that are not addressed by control activities at 3rd Millennium are described within Section 4 and within the 'Subservice Organizations' section above.

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

SECTION 4

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

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

A-LIGN ASSURANCE's examination of the controls of 3rd Millennium was limited to the Trust Services Criteria, related criteria and control activities specified by the management of 3rd Millennium and did not encompass all aspects of 3rd Millennium's operations or operations at user entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) AT-C 105 and AT-C 205.

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

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

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

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

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Core values are communicated from executive management to personnel through policies, procedures, the code of conduct and the employee handbook.	Inspected the employee handbook, 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.	Inspected the signed employee handbook and code of conduct acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
		Upon hire, personnel deemed to have access to sensitive information are required to complete a background check.	Inquired of the Project Director regarding background checks to determine that upon hire, personnel deemed to have access to sensitive information were required to complete a background check.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		An anonymous hotline is in place to allow employees, third parties, and customers to report unethical behavior in a confidential manner.	Inspected the entities website and employee handbook 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.
		Employees, third parties, and customers are directed on how to report unethical behavior in a confidential manner.	Inspected the reporting and escalation policy and the entity's website to determine that employees, third parties, and customers were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Executive management roles and responsibilities are documented and reviewed annually.	Inspected the executive management job descriptions including revision dates to determine that executive management roles and responsibilities were documented and reviewed annually.	No exceptions noted.
		Executive management defines and documents the skills and expertise needed among its members.	Inspected the executive management job descriptions to determine that executive management defined and documented the skills and expertise needed among its members.	No exceptions noted.
		Executive management maintains independence from those that operate the key controls implemented within the environment.	Inspected the organizational chart and the completed internal controls matrix to determine that executive management maintained independence from those that operate the key controls implemented within the environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	Inspected the meeting agenda for internal controls review to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls within the environment.	No exceptions noted.
		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.
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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's shared drive.	Inspected the job description for a sample of job roles 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.	No exceptions noted.
		Executive management reviews job descriptions annually and makes updates, if necessary.	Inspected the revision history of the job description for a sample of job roles to determine that executive management reviewed job descriptions annually and made updates, if necessary.	No exceptions noted.
		Executive management has established proper segregations of duties for key job functions and roles within the organization.	Inspected the organizational chart, the completed internal controls matrix, and job description for a sample of job roles to determine that executive management established proper segregations of duties for key job functions and roles within the organization.	No exceptions noted.
		Roles and responsibilities defined in written job descriptions consider and address specific requirements relevant to the system.	Inspected the job description for a sample of job roles to determine that roles and responsibilities defined in written job descriptions considered and addressed specific requirements relevant to the system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third parties.	Inspected the vendor risk assessment policies and procedures and completed vendor risk assessment to determine that a vendor risk assessment was performed on an annual basis which included reviewing the activities performed by third parties.	No exceptions noted.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Upon hire, personnel deemed to have access to sensitive information are required to complete a background check.	Inquired of the Project Director regarding background checks to determine that upon hire, personnel deemed to have access to sensitive information were required to complete a background check.	No exceptions noted.
			Inspected the employee handbook to determine that upon hire, personnel deemed to have access to sensitive information 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 deemed to have access to sensitive information were required to complete a background check.	Testing of the control activity disclosed that no new hires were deemed to have access to sensitive information 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.	Inspected the employee performance evaluation policies and procedures and competency and training requirements policies and procedures to determine that policies and procedures were in place that outlined the performance evaluation process as well as the competency and training requirements for personnel.	No exceptions noted.
		The entity evaluates the competencies and experience of candidates prior to hiring.	Inspected the resume for a sample of new hires to determine that the entity evaluated the competencies and experience of candidates prior to hiring.	No exceptions noted.
		Employees are required to attend continued training annually that relates to their job role and responsibilities.	Inspected the training completion certificate for a sample of current employees to determine that employees were required to attend security awareness training annually.	No exceptions noted.
		Executive management has created a training program for its employees.	Inspected the information security and awareness training program to determine that executive management created a training program for its employees.	No exceptions noted.
		Management tracks and monitors compliance with information security and awareness training requirements.	Inspected the security awareness training tracker to determine that management tracked and monitored compliance with information security and awareness training requirements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity assesses training needs on an annual basis.	Inspected the training needs assessment to determine that the entity assessed the training needs on an annual basis.	No exceptions noted.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis.	Inspected the signed employee handbook and code of conduct acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook and code of conduct on an annual basis.	No exceptions noted.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
		Sanction policies, which include probation, suspension and termination, are in place for employee misconduct.	Inspected the sanction policies to determine that sanction policies, which include probation, suspension and termination, were in place for employee misconduct.	No exceptions noted.
		A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's shared drive.	Inspected the job description for a sample of job roles 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.	No exceptions noted.
		Executive management reviews job descriptions annually and makes updates, if necessary.	Inspected the revision history of the job description for a sample of job roles to determine that executive management reviewed job descriptions annually and made updates, if necessary.	No exceptions noted.
		Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.	Inspected the employee performance evaluation policies and procedures and competency and training requirements policies and procedures to determine that policies and procedures were in place that outlined the performance evaluation process as well as the competency and training requirements for personnel.	No exceptions noted.
		Executive management reviews the job requirements and responsibilities documented within job descriptions annually and makes updates, if necessary.	Inspected the job descriptions for a sample of job roles including their revision history to determine that executive management reviewed the job requirements and responsibilities documented within job descriptions annually and made updates, if necessary.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Organizational and information security policies and procedures are documented and made available to personnel through the entity's google drive.	Inspected the organizational and information security policies and procedures and the entity's shared drive to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's shared drive.	No exceptions noted.
		Edit checks are in place to prevent incomplete or incorrect data from being entered into the system.	Inspected the edit check configurations to determine that edits checks were in place to prevent incomplete or incorrect data from being entered into the system.	No exceptions noted.
		A data flow diagram is documented and maintained by management to identify the relevant internal and external information sources of the system.	Inspected the data flow diagram to determine that a data flow diagram was documented and maintained by management to identify the relevant internal and external information sources of the system.	No exceptions noted.
		Data entered into the system, processed by the system and output from the system is protected from unauthorized access.	Inspected the system configurations and validation checks to determine that data entered into the system, processed by the system and outputted from the system is reviewed for completeness and accuracy.	No exceptions noted.
		Data is only retained for as long as required to perform the required system functionality, service or use.	Inspected the data management policy to determine that data was retained for only as long as required to perform the required system functionality, service or use.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.	Inspected the signed employee handbook and code of conduct acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
		Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis.	Inspected the signed employee handbook and code of conduct acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook and code of conduct on an annual basis.	No exceptions noted.
		An anonymous hotline is in place to allow employees, third parties, and customers to report unethical behavior in a confidential manner.	Inspected the entities website and employee handbook 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.
		Employees, third parties, and customers are directed on how to report unethical behavior in a confidential manner.	Inspected the reporting and escalation policy and the entity's website to determine that employees, third parties, and customers were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's shared drive.	Inspected the job description for a sample of job roles 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.	No exceptions noted.
		The entity's policies and procedures and employee handbook are made available to personnel through the entity's shared drive.	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 personnel through the entity's shared drive.	No exceptions noted.
		Upon hire, personnel are required to complete information security awareness training.	Inspected the information security awareness training completion form for a sample of new hires to determine that upon hire, personnel were required to complete information security awareness training.	No exceptions noted.
		Current employees are required to complete information security awareness training annually.	Inspected the information security awareness training completion form for a sample of current employees to determine that current employees were required to complete information security awareness training annually.	No exceptions noted.
		Executive management meets annually with operational management to discuss the entity's objectives as well as roles and responsibilities.	Inspected the meeting agenda for internal controls review to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls within the environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Changes to job roles and responsibilities are communicated to personnel through the entity's shared drive.	Inspected the entity's shared drive to determine that changes to job roles and responsibilities were communicated to personnel through the entity's shared drive.	No exceptions noted.
		Documented escalation procedures for reporting failures, incidents, concerns and other complaints are in place and made available to personnel through the entity's shared drive.	Inspected the reporting and escalation 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 personnel through the entity's shared drive.	No exceptions noted.
		The entity's objectives, including changes made to the objectives, are communicated to its personnel through the entity's shared drive.	Inspected the entity's shared drive to determine that the entity's objectives, including changes made to the objectives, were communicated to its personnel through the entity's shared drive.	No exceptions noted.
		The information security policies and procedures that communicate the system commitments and requirements of external users are provided to external users prior to allowing them access to the system.	Inspected the information security policies and procedures to determine that the information security policies and procedures that communicated the system commitments and requirements of external users were provided to external users prior to allowing them access to the system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	An anonymous hotline is in place to allow employees, third parties, and customers to report unethical behavior in a confidential manner.	Inspected the entities website and employee handbook 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.
		Employees, third parties, and customers are directed on how to report unethical behavior in a confidential manner.	Inspected the reporting and escalation policy and the entity's website to determine that employees, third parties, and customers were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.
		Documented escalation procedures for reporting failures, incidents, concerns and other complaints are in place and made available to personnel through the entity's shared drive.	Inspected the reporting and escalation 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 personnel through the entity's shared drive.	No exceptions noted.
		The entity's third-party agreements delineate the boundaries of the system and describe relevant system components.	Inspected the third-party agreement for a sample of third parties to determine that the entity's third-party agreement delineated the boundaries of the system and described relevant system components.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity's third-party agreement communicates the system commitments and requirements of third parties.	Inspected the third-party agreement for a sample of third parties to determine that the entity's third-party agreement communicated the system commitments and requirements of third parties.	No exceptions noted.
		The entity's third-party agreement outlines and communicates the terms, conditions and responsibilities of third parties.	Inspected the third-party agreement for a sample of third parties to determine that the entity's third-party agreement outlined and communicated the terms, conditions and responsibilities of third parties.	No exceptions noted.
		The entity's contractor agreement outlines and communicates the terms, conditions and responsibilities of external users.	Inspected the contractor agreement template to determine that the entity's contractor agreement outlined and communicated the terms, conditions and responsibilities of external users.	No exceptions noted.
		Changes to commitments, requirements and responsibilities are communicated to third parties, external users, and customers via website notices	Inspected the entity's website to determine that changes to commitments, requirements and responsibilities were communicated to third parties, external users and customers website notices.	No exceptions noted.
		Executive management meets annually with operational management to discuss the results of assessments performed by third parties.	Inspected the meeting agenda for internal controls review to determine that executive management met annually with operational management to discuss the results of assessments performed by third parties.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
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 evaluation policies and procedures and the entity's documented objectives and strategies to determine that the entity established organizational strategies and objectives that were used to determine entity structure and performance metrics.	No exceptions noted.
		Executive management has documented objectives that are specific, measurable, attainable, relevant and time-bound (SMART).	Inspected the entity's documented objectives and strategies to determine that executive management had documented objectives that were specific, measurable, attainable, relevant and time-bound (SMART).	No exceptions noted.
		Executive management identifies and assesses risks that could prevent the entity's objectives from being achieved.	Inspected the risk assessment and management policies and procedures and completed risk assessment to determine that executive management identified and assessed risks that could prevent the entity's objectives from being achieved.	No exceptions noted.
		Executive management has established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	Inspected the documented key performance indicators for operational and internal controls effectiveness to determine that executive management established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Responsible parties are defined and assigned to coordinate and monitor compliance and audit activities.	Inspected the organizational chart and project director job description to determine that responsible parties were defined and assigned to coordinate and monitor compliance and audit activities.	No exceptions noted.
		The entity has defined the desired level of performance and operation in order to achieve the established entity objectives.	Inspected the documented key performance indicators for operational and internal controls effectiveness to determine that the entity defined the desired level of performance and operation in order to achieve the established entity objectives.	No exceptions noted.
		Key performance indicators of both the business performance and employee performance are developed in alignment with entity objectives and strategies.	Inspected the employee performance evaluation policies and procedures, the entity's documented objectives and strategies and the documented key performance indicators for operational and internal controls effectiveness to determine that key performance indicators of both the business performance and employee performance were developed in alignment with entity objectives and strategies.	No exceptions noted.
		Business plans and budgets align with the entity's strategies and objectives.	Inspected the entity's business plans, budget, and documented objectives and strategies to determine that business plans and budgets aligned with the entity's strategies and objectives.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Entity strategies, objectives and budgets are assessed on an annual basis.	Inspected the management meeting minutes to determine that entity strategies, objectives and budgets were assessed on an annual basis.	No exceptions noted.
		The entity's internal controls framework is based on a recognized (NIST 800-53; COBIT; ISO; COSO) framework.	Inspected the internal controls matrix to determine that the entity's internal controls framework was based on a recognized framework.	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 and management policies and procedures to determine that documented policies and procedures were in place to guide personnel when performing a risk assessment.	No exceptions noted.
		Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	Inspected the risk assessment and management policies and procedures to determine that management defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	No exceptions noted.
		A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.

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

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

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Identified fraud risks are reviewed and addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the completed fraud assessment to determine that identified fraud risks were reviewed and addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
		As part of management's assessment of fraud risks, management considers key fraud factors such as incentives, pressures, opportunity for unauthorized access or use of data, and employee morale and attitude.	Inspected the completed fraud assessment to determine that as part of management's assessment of fraud risks, management considered key fraud factors such as incentives, pressures, opportunity for unauthorized access or use of data, and employee morale and attitude.	No exceptions noted.
		As part of management's assessment of fraud risks, management considers how personnel could engage in or justify fraudulent activities.	Inspected the completed fraud assessment to determine that as part of management's assessment of fraud risks, management considered how personnel could engage in or justify fraudulent activities.	No exceptions noted.
		As part of management's assessment of fraud risks, management considers threats and vulnerabilities that arise from the use of IT.	Inspected the completed fraud assessment to determine that as part of management's assessment of fraud risks, management considered threats and vulnerabilities that arise from the use of IT.	No exceptions noted.

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

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		On an annual basis, management reviews the controls implemented within the environment for compliance and operational effectiveness and identifies potential control gaps and weaknesses.	Inspected the meeting agenda for internal controls review 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.
		Control self-assessments that include, but are not limited to, physical and logical access reviews, and backup restoration tests are performed on at least an annual basis.	Inspected the completed backup restoration test and the completed access review to determine that control self-assessments that included, but were not limited to, physical and logical access reviews, and backup restoration tests were performed on at least an annual basis.	No exceptions noted.
		A data backup restoration test is performed on an annual basis.	Inspected the completed backup restoration test ticket to determine that a data backup restoration test was performed on an annual basis.	No exceptions noted.
		Internal and external vulnerability scans and penetration tests are performed on at least an annual basis and remedial actions are taken where necessary.	Inspected the completed vulnerability scan results and the completed penetration test results to determine that internal and external vulnerability scans and penetration tests were performed on at least an annual basis and remedial actions were taken where necessary.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A third-party performs a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	Inspected the completed penetration test results to determine that a third-party performed a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	No exceptions noted.
		Management obtains and reviews attestation reports and vendor questionnaires of vendors and third parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Inspected the completed third-party attestation reports review for a sample of third parties that the entity has a relationship with 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.
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.	Senior management assesses the results of the compliance, control and risk assessments performed on the environment.	Inspected the meeting agenda for internal controls review to determine that senior management assessed the results of the compliance, control and risk assessments performed on the environment.	No exceptions noted.
		Senior management is made aware of high-risk vulnerabilities, deviations and controls gaps identified as part of the compliance, control and risk assessments performed.	Inspected the meeting agenda for internal controls review to determine that senior management was made aware of high-risk vulnerabilities, deviations and controls gaps identified as part of the compliance, control and risk assessments performed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment are communicated to those parties responsible for taking corrective actions.	Inspected the completed risk assessment to determine that vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment were communicated to those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the supporting ticket for a sample of vulnerabilities identified from a penetration test to determine that vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment were communicated to those parties responsible for taking corrective actions.	No exceptions noted.
		Vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment are documented, investigated, and addressed.	Inspected the completed risk assessment to determine that vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment were documented, investigated, and addressed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting ticket for a sample of vulnerabilities identified from a penetration test to determine that vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment were documented, investigated, and addressed.	No exceptions noted.
		Management tracks whether vulnerabilities, deviations and control failures/gaps identified as part of the evaluations performed are addressed in a timely manner.	Inspected the supporting incident ticket for a sample of vulnerabilities identified to determine that management tracked whether vulnerabilities, deviations and control gaps identified as part of the evaluations performed were addressed in a timely manner.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	Inspected the risk assessment and management policies and procedures, completed risk assessment, and associated incident ticket for an example internal control that had failed to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
		As part of the risk assessment process, controls within the environment are modified and implemented to mitigate identified vulnerabilities, deviations and control gaps.	Inspected the completed risk assessment to determine that as part of the risk assessment process, controls within the environment were modified and implemented to mitigate identified vulnerabilities, deviations and control gaps.	No exceptions noted.
		Controls within the environment are modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations (e.g. risk assessments, vulnerability scans) 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 (e.g. risk assessments, vulnerability scans) performed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting ticket for a sample of vulnerabilities identified from a penetration test to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations (e.g. risk assessments, vulnerability scans) 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 completed internal controls matrix to determine that management documented the relevant controls in place for each key business or operational process.	No exceptions noted.
		Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	Inspected the completed internal controls matrix to determine that management incorporated a variety of controls into their environment that included manual, automated, preventive, detective, and corrective controls.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management has documented the relationship and linkage between business processes, the relevant technologies used to support the business processes, and the controls in place to help secure those business processes.	Inspected the completed internal controls matrix to determine that management documented the relationship and linkage between business processes, the relevant technologies used to support the business processes, and the controls in place to help secure those business processes.	No exceptions noted.
		Management has documented the controls implemented around the entity's technology infrastructure.	Inspected the completed internal controls matrix to determine that management documented the controls implemented around the entity's technology infrastructure.	No exceptions noted.
		Management has established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.	Inspected the completed internal controls matrix to determine that management established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.	No exceptions noted.
		As part of the risk assessment process, the use of technology in business processes is evaluated by management.	Inspected the completed risk assessment to determine that as part of the risk assessment process, the use of technology in business processes was evaluated by management.	No exceptions noted.

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

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

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 the completed internal controls matrix to determine that process owners and management operated the controls implemented within the entity's environment based on the frequency defined in the organizational and information security policies and procedures.	No exceptions noted.
		Process owners and management investigate and troubleshoot control failures.	Inspected the completed risk assessment and associated incident ticket for an example internal control that had failed to determine that process owners and management investigated and troubleshot control failures.	No exceptions noted.
		The effectiveness of the internal controls implemented within the environment is evaluated annually.	Inspected the meeting minutes to determine that the effectiveness of the internal controls implemented within the environment was evaluated annually.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the network administrator listing and access rights to determine that network administrative access was restricted to authorized personnel.	No exceptions noted.
		Network users are authenticated via individually-assigned user accounts and passwords.	Inspected the network user listings and password authentication settings to determine that network users were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.
		Networks are configured to enforce password requirements that include: • Minimum Password length • Strong password • 2-Step Verification	Inspected the network password settings to determine that networks were configured to enforce password requirements that included: • Minimum Password length • Strong password • 2-Step Verification	No exceptions noted.
		Network audit logging settings are in place that include: • Account logon events	Inspected the network audit logging settings and an example network audit log extract to determine that network audit logging configurations were in place that included: • Account logon events	No exceptions noted.
		Network audit logs are maintained for review when needed.	Inquired of the Project Director regarding network audit logs to determine that network audit logs were maintained and reviewed as-needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected an example network audit log extract to determine that network audit logs were maintained and reviewed as-needed.	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.
		Operating system administrative access is restricted to authorized personnel.	Inquired of the Project Director regarding operating system administrative access to determine that operating system administrative access was restricted to authorized personnel.	No exceptions noted.
			Inspected the operating system administrator listing to determine that operating system administrative access was restricted to authorized personnel.	No exceptions noted.
		Production server users are authenticated via individually-assigned user accounts and passwords.	Observed a user login to the production servers to determine that production server users were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.
			Inspected the production server password and authentication settings to determine that production servers users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Networks are configured to enforce password requirements that include: • Minimum Password length • Strong password • 2-Step Verification	Inspected the network password settings to determine that networks were configured to enforce password requirements that included: • Minimum Password length • Strong password • 2-Step Verification	No exceptions noted.
		Operating system audit logging configurations are in place.	Inspected the operating system audit logging settings and an example operating system audit log extract to determine that operating system audit logging configurations were in place.	No exceptions noted.
		Operating system audit logs are maintained and reviewed as-needed.	Inquired of the Project Director regarding operating system audit logs to determine that operating system audit logs were maintained and reviewed as-needed.	No exceptions noted.
			Inspected an example operating system log audit extract to determine that operating system audit logs were maintained and reviewed as-needed.	No exceptions noted.
		Database user access is restricted via role-based security privileges defined within the access control system.	Inspected the database user listing and access rights to determine that database user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Database administrative access is restricted to user accounts accessible by authorized personnel.	Inquired of the Project Director regarding database administrative access to determine that database administrative access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
			Inspected the database administrator listing and access rights to determine that database administrative access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		Production database users are authenticated via individually-assigned user accounts and passwords.	Inspected the production database user listings and password configurations to determine that production databases users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
		Database audit logging settings are in place.	Inspected the database audit logging settings and an example database audit log extract to determine that database audit logging configurations were in place.	No exceptions noted.
		Database audit logs are maintained and reviewed as-needed.	Inquired of the Project Director regarding database audit logs to determine that the database audit logs were maintained and reviewed as-needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected an example database audit log extract to determine that database audit logs were maintained and reviewed as-needed.	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.
		Application administrative access is restricted to user accounts accessible by authorized personnel.	Inquired of the Project Director regarding application administrative access to determine that application administrative access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
			Inspected the application administrator listing and access rights to determine that application administrative access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		The application is configured to enforce password requirements that include: • Password length • Complexity	Inspected the application password settings to determine that application was configured to enforce password requirements that included: • Password length • Complexity	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Application audit logging settings are in place.	Inspected the application audit logging settings and an example application audit log extract to determine that application audit logging configurations were in place.	No exceptions noted.
		Application audit logs are maintained and reviewed as-needed.	Inquired of the Project Director regarding application audit logs to determine that application audit logs were maintained and reviewed as-needed.	No exceptions noted.
			Inspected an example application audit log extract to determine that application audit logs were maintained and reviewed as-needed.	No exceptions noted.
		VPN user access is restricted via role-based security privileges defined within the access control system.	Inspected the VPN user listing and access rights to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		The ability to administer VPN access is restricted to authorized personnel.	Inspected the VPN administrator listing to determine that the ability to administer VPN access was restricted to authorized personnel.	No exceptions noted.
		The entity's various networks are segmented to keep information and data isolated and restricted to authorized personnel.	Inspected the network segmentation documentation to determine that the entity's various networks were segmented to keep information and data isolated and restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		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.
		Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.	Inspected the encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.
		Critical data is stored in encrypted format using advanced encryption standard (AES).	Inspected the encryption configurations for data at rest to determine that critical data was stored in encrypted format using AES.	No exceptions noted.
		Control self-assessments that include physical and logical access reviews are performed on at least an annual basis.	Inspected the completed user access review to determine that control self-assessments that included physical and logical access reviews were performed on at least an annual basis.	No exceptions noted.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inspected the hiring procedures, user access listings and user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Logical access to systems is revoked for an employee as a component of the termination process.	Inspected the termination procedures, user access listings 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.	No exceptions noted.
		Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the Project Director regarding privileged access to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
			Inspected the listings of privileged users to the network, operating system, database and application to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
		Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the Project Director regarding privileged access to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the listings of privileged users to the network, operating system, database and application to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
		Control self-assessments that include physical and logical access reviews are performed on at least an annual basis.	Inspected the completed user access review to determine that control self-assessments that included physical and logical access reviews were performed on at least an annual basis	No exceptions noted.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inspected the hiring procedures, user access listings and user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked for an employee as a component of the termination process.	Inspected the termination procedures, user access listings 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.	No exceptions noted.
		Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the Project Director regarding privileged access to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the listings of privileged users to the network, operating system, database and application to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	An analysis of incompatible operational duties is performed on at least an annual basis, and where incompatible responsibilities are identified, compensating controls are put into place.	Inspected the organizational chart and internal controls matrix to determine that an analysis of incompatible operational duties was performed on at least an annual basis, and where incompatible responsibilities were identified, compensating controls were put into place.	No exceptions noted.
		Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
		Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the Project Director regarding privileged access to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
			Inspected the listings of privileged users to the network, operating system, database and application to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.

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

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Logical access to systems is revoked for an employee as a component of the termination process.	Inspected the termination procedures, user access listings 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.	No exceptions noted.
		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.
		Part of this criterion is the responsibility of the subservice organization. Refer to the "Subservice Organizations" section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	Policies and procedures are in place to guide personnel in data, hardware and software disposal and destruction.	Inspected the data disposal and destruction policies and procedures to determine that policies and procedures were in place to guide personnel in data, hardware and software disposal and destruction.	No exceptions noted.
		The entity purges data stored on backups as necessary.	Inquired of the Project Director regarding data disposals to determine that the entity purged data stored on backups as necessary.	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 data disposal policies and procedures to determine that the entity purged data stored on backups as necessary.	No exceptions noted.
			Inspected the supporting ticket for a sample of data disposal requests to determined that the entity purged data stored on backups as necessary.	Testing of the control activity disclosed that no data disposals occurred during the review period.
		Data that is no longer required is disposed of and rendered unreadable to meet the entity's objectives.	Inquired of the Project Director regarding data disposals to determine that data that was no longer required was disposed of and rendered unreadable to meet the entity's objectives.	No exceptions noted.
			Inspected the data disposal policies and procedures to determine that data that was no longer required was disposed of and rendered unreadable to meet the entity's objectives.	No exceptions noted.
			Inspected the supporting ticket for a sample of data disposal requests to determine that data that was no longer required was disposed of and rendered unreadable to meet the entity's objectives.	Testing of the control activity disclosed that no data disposals occurred during the review period.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	VPN user access is restricted via role-based security privileges defined within the access control system.	Inspected the VPN user listing and access rights to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.	Inspected the encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.
		Critical data is stored in encrypted format using advanced encryption standard (AES).	Inspected the encryption configurations for data at rest to determine that critical data was stored in encrypted format using AES.	No exceptions noted.
		Network address translation (NAT) functionality is utilized to manage internal IP addresses.	Inspected the NAT configurations to determine that NAT functionality was utilized to manage internal IP addresses.	No exceptions noted.
		TLS and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations and digital certificates to determine that TLS and other encryption technologies were used for defined points of connectivity.	No exceptions noted.
		Logical access to stored data is restricted to authorized personnel.	Inquired of the Project Director regarding logical access to stored data to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
			Inspected the database user listing and access rights to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the network diagram and firewall rulesets to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram and firewall rulesets 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 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 example IDS extract and alert notification to determine that the IDS was configured to notify personnel upon intrusion detection.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Antivirus software is installed on workstations and servers to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus configurations for a sample of workstations 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 is configured to scan workstations on a weekly basis.	Inspected the antivirus configurations for a sample of workstations to determine that the antivirus software was configured to scan workstations on a weekly basis.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.	Inspected the encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.
		Critical data is stored in encrypted format using advanced encryption standard (AES).	Inspected the encryption configurations for data at rest to determine that critical data was stored in encrypted format using AES.	No exceptions noted.
		Network address translation (NAT) functionality is utilized to manage internal IP addresses.	Inspected the NAT configurations to determine that NAT functionality was utilized to manage internal IP addresses.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		TLS and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations and digital certificates to determine that TLS and other encryption technologies were used for defined points of connectivity.	No exceptions noted.
		Logical access to stored data is restricted to authorized personnel.	Inquired of the Project Director regarding logical access to stored data to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
			Inspected the database user listing and access rights to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the network diagram and firewall rulesets to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram and firewall rulesets 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 utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			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 example IDS extract and alert notification to determine that the IDS was configured to notify personnel upon intrusion detection.	No exceptions noted.
		The ability to restore backups is restricted to authorized personnel.	Inspected the listing of users with the ability to restore backups to determine that the ability to restore backups was restricted to authorized personnel.	No exceptions noted.
		Backup data is replicated offsite by a third-party vendor weekly.	Inspected the contract with the offsite backup storage vendor to determine that backup media was replicated offsite by a third-party vendor weekly.	No exceptions noted.
		Backup media is stored in an encrypted format.	Inspected the encryption policy to determine that backup media was stored in an encrypted format.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Antivirus software is installed on workstations and servers to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus configurations for a sample of workstations 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 is configured to scan workstations on a weekly basis.	Inspected the antivirus configurations for a sample of workstations to determine that the antivirus software was configured to scan workstations on a weekly basis.	No exceptions noted.
		The ability to migrate changes into the production environment is restricted to authorized and appropriate users.	Inquired of the Project Director regarding the ability to migrate changes 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.
		File integrity monitoring (FIM) software is in place to ensure only authorized changes are deployed into the production environment.	Inspected the FIM configurations to determine that FIM software was in place to ensure only authorized changes are deployed into the production environment.	No exceptions noted.
		The code repository is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected the code repository notification configurations and an example alert generated from the code repository to determine that the code repository was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Documented change control policies and procedures are in place to guide personnel in the change management process.	Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in the change management process.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram and firewall rulesets 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 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 example IDS extract and alert notification to determine that the IDS was configured to notify personnel upon intrusion detection.	No exceptions noted.
		File integrity monitoring (FIM) software is in place to ensure only authorized changes are deployed into the production environment.	Inspected the FIM configurations to determine that FIM software was in place to ensure only authorized changes are deployed into the production environment.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, FIM configurations, IDS configurations, IPS configurations, and firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		Network audit logging settings are in place that include: • Account logon events	Inspected the network audit logging settings and an example network audit log extract to determine that network audit logging configurations were in place that included: • Account logon events	No exceptions noted.
		Network audit logs are maintained for review when needed.	Inquired of the Project Director regarding network audit logs to determine that network audit logs were maintained and reviewed as-needed.	No exceptions noted.
			Inspected an example network audit log extract to determine that network audit logs were maintained and reviewed as-needed.	No exceptions noted.
		Operating system audit logging configurations are in place.	Inspected the operating system audit logging settings and an example operating system audit log extract to determine that operating system audit logging configurations were in place.	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**
		Operating system audit logs are maintained and reviewed as-needed.	Inquired of the Project Director regarding operating system audit logs to determine that operating system audit logs were maintained and reviewed as-needed.	No exceptions noted.
			Inspected an example operating system log audit extract to determine that operating system audit logs were maintained and reviewed as-needed.	No exceptions noted.
		Database audit logging settings are in place.	Inspected the database audit logging settings and an example database audit log extract to determine that database audit logging configurations were in place.	No exceptions noted.
		Database audit logs are maintained and reviewed as-needed.	Inquired of the Project Director regarding database audit logs to determine that the database audit logs were maintained and reviewed as-needed.	No exceptions noted.
			Inspected an example database audit log extract to determine that database audit logs were maintained and reviewed as-needed.	No exceptions noted.
		Application audit logging settings are in place.	Inspected the application audit logging settings and an example application audit log extract to determine that application audit logging configurations were in place.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Application audit logs are maintained and reviewed as-needed.	Inquired of the Project Director regarding application audit logs to determine that application audit logs were maintained and reviewed as-needed.	No exceptions noted.
			Inspected an example application audit log extract to determine that application audit logs were maintained and reviewed as-needed.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organization. Refer to the “Subservice Organizations” section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
		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 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 example IDS extract and alert notification to determine that the IDS was configured to notify personnel upon intrusion detection.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Antivirus software is installed on workstations and servers to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus configurations for a sample of workstations 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 is configured to scan workstations on a weekly basis.	Inspected the antivirus configurations for a sample of workstations to determine that the antivirus software was configured to scan workstations on a weekly basis.	No exceptions noted.
		File integrity monitoring (FIM) software is in place to ensure only authorized changes are deployed into the production environment.	Inspected the FIM configurations to determine that FIM software was in place to ensure only authorized changes are deployed into the production environment.	No exceptions noted.
		The code repository is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected the code repository notification configurations and an example alert generated from the code repository to determine that the code repository was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
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, an example log extract from the IDS and an example IDS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.
		Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected the information security and incident policies and procedures to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	No exceptions noted.
		Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident management and escalation policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management reviews reports on an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes.	Inspected the meeting minutes to determine that management reviewed reports on an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identified the need for system changes and implementation of additional controls based on incident patterns and root causes.	No exceptions noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident management and escalation policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		The incident response and escalation procedures are reviewed at least annually for effectiveness.	Inspected the revision history of the incident response policies and procedures to determine that the incident response and escalation procedures were reviewed at least annually for effectiveness.	No exceptions noted.
		The incident response policies and procedures define the classification of incidents based on its severity.	Inspected the incident response policies and procedures to determine that the incident response policies and procedures defined the classification of incidents based on its severity.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Resolution of incidents are documented within the ticket and communicated to affected users.	Inspected the supporting incident ticket for a sample of incidents to determine that resolution of incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inspected the supporting incident ticket for a sample of incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
		A security incident analysis is performed for incidents to determine the root cause, system impact and resolution.	Inspected the security incident analysis for a sample of security incidents to determine that a security incident analysis was performed for incidents to determine the root cause, system impact and resolution.	No exceptions noted.
		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 determination and execution of the containment approach.	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 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.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident management and escalation policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		Management reviews reports on an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes.	Inspected the meeting minutes to determine that management reviewed reports on an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identified the need for system changes and implementation of additional controls based on incident patterns and root causes.	No exceptions noted.

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 and escalation procedures are reviewed at least annually for effectiveness.	Inspected the revision history of the incident response policies and procedures to determine that the incident response and escalation procedures were reviewed at least annually for effectiveness.	No exceptions noted.
		Resolution of incidents are documented within the ticket and communicated to affected users.	Inspected the supporting incident ticket for a sample of incidents to determine that resolution of incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inspected the supporting incident ticket for a sample of incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
		A security incident analysis is performed for incidents to determine the root cause, system impact and resolution.	Inspected the security incident analysis for a sample of security incidents to determine that a security incident analysis was performed for incidents to determine the root cause, system impact and resolution.	No exceptions noted.
		Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are defined and documented.	Inspected the incident response policies and procedures to determine that roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program were defined and documented.	No exceptions noted.

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 actions taken to address identified security incidents are documented and communicated to affected parties.	Inspected the supporting incident ticket for a sample of incidents to determine that the actions taken to address identified security incidents were documented and communicated to affected parties.	No exceptions noted.
		Documented incident response and escalation procedures are in place to guide personnel in addressing the threats posed by security incidents.	Inspected the incident response policies and procedures to determine that documented incident response and escalation procedures were in place to guide personnel in addressing the threats posed by security incidents.	No exceptions noted.
		Critical security incidents that result in a service/business operation disruption are communicated to those affected through e-mails.	Inquired of the Project Director regarding critical security incidents to determine that critical security incidents that resulted in a service/business operation disruption were communicated to those affected through e-mails.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that critical security incidents that resulted in a service/business operation disruption were communicated to those affected through e-mails.	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 an example critical security incident that resulted in a service/business operation disruption to determine that critical security incidents that result in a service/business operation disruption were communicated to those affected through e-mails.	Testing of the control activity disclosed that no critical security incidents occurred during the review period.
		Remediation actions taken for security incidents are documented within the ticket and communicated to affected users.	Inspected the supporting incident ticket for a sample of incidents to determine that the remediation actions taken for security incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
		The risks associated with identified vulnerabilities are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the supporting incident ticket for a vulnerability identified from a vulnerability scan or penetration test and completed risk assessment to determine that the risks associated with identified vulnerabilities were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	A data backup restoration test is performed on an annual basis.	Inspected the completed backup restoration test ticket to determine that a data backup restoration test was performed on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed business continuity and disaster recovery test results to determine that the business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.
		Management reviews reports on an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes.	Inspected the meeting minutes to determine that management reviewed reports on an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identified the need for system changes and implementation of additional controls based on incident patterns and root causes.	No exceptions noted.
		A security incident analysis is performed for incidents to determine the root cause, system impact and resolution.	Inspected the security incident analysis for a sample of security incidents to determine that a security incident analysis was performed for incidents to determine the root cause, system impact and resolution.	No exceptions noted.
		Change management requests are opened for incidents that require permanent fixes.	Inspected the change management policies and procedures and the change ticket for an example incident that required a permanent fix to determine that change management requests were required to be opened for incidents that required permanent fixes.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity restores system operations for incidents impacting the environment through activities that include, but are not limited to: • Rebuilding systems • Updating software • Installing patches • Removing unauthorized access • Changing configurations	Inspected the information security, incident, and change management policies and procedures, and the system build guides for critical systems to determine that the entity restored system operations for incidents impacting the environment through activities that included, but were not limited to: • Rebuilding systems • Updating software • Installing patches • Removing unauthorized access • Changing configurations	No exceptions noted.
		Data backup and restore procedures are in place to guide personnel in performing backup activities.	Inspected the backup policies and procedures to determine that data backup and restore procedures were in place to guide personnel in performing backup activities.	No exceptions noted.
		A business continuity and disaster recovery plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	Inspected the business continuity and disaster recovery plans to determine that a business continuity and disaster recovery plan was documented to identify and reduce risks, limited the consequences of damaging incidents, and ensured the timely resumption of essential operations.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The ability to migrate changes into the production environment is restricted to authorized and appropriate users.	Inquired of the Project Director regarding the ability to migrate changes 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.
		File integrity monitoring (FIM) software is in place to ensure only authorized changes are deployed into the production environment.	Inspected the FIM configurations to determine that FIM software was in place to ensure only authorized changes are deployed into the production environment.	No exceptions noted.
		The code repository is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected the code repository notification configurations and an example alert generated from the code repository to determine that the code repository was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.
		Documented change control policies and procedures are in place to guide personnel in the change management process.	Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in the change management process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The change management process has defined the following roles and assignments: • Authorization of change requests - 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 e-mails to determine that system changes were communicated to both affected internal and external users.	No exceptions noted.
		System changes are authorized and approved by management prior to implementation.	Inspected the supporting change ticket for a sample of system changes to determine that system changes were authorized and approved by management prior to implementation.	No exceptions noted.
		Prior code is held in the source code repository for rollback capability in the event that a system change does not function as designed.	Inspected the change control software settings to determine that prior code was held in the source code repository for rollback capability in the event that a system change did not function as designed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		System patches/security updates follow the standard change management process.	Inspected the patch management policies and procedures to determine that system patches/security updates follow the standard patch management process.	No exceptions noted.
		Development and test environments are physically and logically separated from the production environment.	Inspected the separate development, QA and production environments to determine that development and test environments were physically and logically separated from the production environment.	No exceptions noted.
		System change requests are documented and tracked in a ticketing system.	Inspected the supporting change ticket for a sample of system changes to determine that system change requests were documented and tracked in a ticketing system.	No exceptions noted.
		Back out procedures are documented to allow for rollback of application changes when changes impaired system operations.	Inspected the supporting change ticket for a sample of system changes to determine that back out procedures were documented within each change implementation to allow for rollback of changes when changes impair system operation.	No exceptions noted.
		A code/peer review is systematically required prior to deploying the PR into the production environment.	Inspected the supporting change ticket for a sample of network, system, and application changes to determine that a code/peer review was systematically required prior to deploying the PR into the production environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		System changes are tested prior to implementation. Types of testing performed depend on the nature of the change.	Inspected the supporting change ticket for a sample of system changes to determine that system changes were authorized and approved by management prior to implementation.	No exceptions noted.
		System changes implemented for remediating incidents follow the standard change management process.	Inspected the change management policies and procedures to determine that system changes implemented for remediating incidents followed the standard change management process.	No exceptions noted.
			Inspected the supporting change ticket for a sample of system changes to determine that system changes implemented for remediating incidents followed the standard change management process.	No exceptions noted.
		Information security policies and procedures document the baseline requirements for configuration of IT systems and tools.	Inspected the information security policies and procedures to determine that information security policies and procedures documented the baseline requirements for configuration of IT systems and tools.	No exceptions noted.
		Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency situation.	Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in implementing changes in an emergency situation.	No exceptions noted.

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

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

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

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

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

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