A-LIGN

Unravel Data

Type 2 SOC 2

2023

unravel™

REPORT ON UNRAVEL DATA'S DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS RELEVANT TO SECURITY

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

January 1, 2023 to December 31, 2023

Table of Contents

SECTION 1

ASSERTION OF UNRAVEL DATA MANAGEMENT

ASSERTION OF UNRAVEL DATA MANAGEMENT

January 5, 2024

We have prepared the accompanying description of Unravel Data's ('Unravel' or 'the Company') Powered Performance Management Software Services System titled "Unravel Data's Description of Its Powered Performance Management Software Services System throughout the period January 1, 2023 to December 31, 2023" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the Powered Performance Management Software Services System that may be useful when assessing the risks arising from interactions with Unravel's system, particularly information about system controls that Unravel 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*).

Unravel uses Amazon Web Services, Inc. ('AWS'), Google Cloud Platform ('GCP'), and Microsoft Azure ('Azure') to provide cloud hosting services (collectively, the 'subservice organizations'). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Unravel, to achieve Unravel's service commitments and system requirements based on the applicable Trust Services Criteria. The description presents Unravel's controls, the applicable Trust Services Criteria, and the types of complementary subservice organization controls assumed in the design of Unravel's controls. The description does not disclose the actual controls at the subservice organizations.

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

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

a. the description presents Unravel's Powered Performance Management Software Services System that was designed and implemented throughout the period January 1, 2023 to December 31, 2023, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that Unravel'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 Unravel's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that Unravel'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 Unravel's controls operated effectively throughout that period.

Kunal Agarwal
Chief Executive Officer
Unravel Data

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Unravel Data

Scope

We have examined Unravel's accompanying description of its Powered Performance Management Software Services System titled "Unravel Data's Description of Its Powered Performance Management Software Services System throughout the period January 1, 2023 to December 31, 2023" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that Unravel'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*).

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

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

Unravel 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 Unravel's service commitments and system requirements were achieved. Unravel has provided the accompanying assertion titled "Assertion of Unravel Data Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Unravel 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 Unravel's Powered Performance Management Software Services System that was designed and implemented throughout the period January 1, 2023 to December 31, 2023, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that Unravel'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 Unravel's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that Unravel'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 Unravel'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 Unravel, user entities of Unravel's Powered Performance Management Software Services System during some or all of the period January 1, 2023 to December 31, 2023, business partners of Unravel subject to risks arising from interactions with the Powered Performance Management Software Services System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

A-LIGN ASSURANCE

Tampa, Florida
January 5, 2024

SECTION 3

UNRAVEL DATA'S DESCRIPTION OF ITS POWERED PERFORMANCE MANAGEMENT SOFTWARE SERVICES SYSTEM THROUGHOUT THE PERIOD JANUARY 1, 2023 TO DECEMBER 31, 2023

OVERVIEW OF OPERATIONS

Company Background

Unravel was founded in 2013 with the objective of simplifying modern data application performance and operations. The company has raised $57M from top tier Venture Capitals like Menlo Ventures and Grantie Global Ventures (GGV) Capital. The organization is based in Palo Alto, California, with an office in Bangalore, India.

Description of Services Provided

Unravel's software solution (the "Software") is application performance management (APM) software. The Software provides monitoring and analytics to offer actionable recommendations and automation for tuning, troubleshooting, and improving performance with respect to various applications within a customer's computing environment(s). Unravel Software is downloadable software that is installed and implemented within customer-controlled computing environments (whether on-prem, in the cloud, or hybrid).

Unravel also provides support and maintenance ("Support") to customers for the Unravel Software, where customers can obtain troubleshooting, bug fixes and other assistance relating to their installation, implementation and use of the Unravel Software. Support is provided via an online portal and is provided by Unravel personnel in the United States and India.

Principal Service Commitments and System Requirements

The systems described herein are the systems that are used to develop and deliver the Unravel Software and Support to customers, and the supporting Information Technology (IT) infrastructure and business processes.

Unravel makes the following commitments to its customers:

- Deliver Unravel support in accordance with Unravel's Support Policy
- Maintain reasonable administrative, technical and physical safeguards to protect confidential information received by Unravel
- Ensure that its information security program and safeguards are designed, maintained, updated and adjusted, as necessary, to protect against reasonably foreseeable internal and external risks to the security, confidentiality and integrity of customer confidential information

These commitments and any others are documented in Unravel's customer agreements.

Components of the System

Infrastructure

Primary infrastructure used to provide Unravel's Powered Performance Management Software Services System includes the following:

Primary Infrastructure		
Hardware	**Platform**	**Purpose**
Unravel laptops	Windows, Mac	Employee workstations
Unravel offices	N/A	Physical locations (United States, Europe and India)
Firewall / Intrusion Prevention System (IPS)	Juniper Secure Services Gateway140 Firewall	Protection for the Unravel datacenter network

Primary Infrastructure		
Hardware	**Platform**	**Purpose**
Virtual Private Network (VPN)	Cisco ASA5520	Secure access to datacenters network
Switches	Cisco	Interconnecting datacenter servers
Servers	Servers from HP, Dell, International Business Machines Corporation (IBM), and other vendors	Unravel servers in the lab where Virtual Machines (VMs) and clusters are hosted

Software

Primary software used to provide Unravel's Powered Performance Management Software Services System, and related support services, includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Salesforce.com	Software as a Service (SaaS) Platform	Customer relationship management tool. Support-related portal hosting provider and provisioning and support ticketing system. Hosted by Salesforce.com
Carbon Black	Antivirus	Antivirus protection for Unravel computing assets
Google Workspace	Google	E-mail & file storage
GitHub	SaaS Platform	Unravel code base
Confluence	Atlassian	Wiki page for internal engineering documentation
Jira	Atlassian	Ticketing system
ExaVault	SaaS Platform	Support-related log files uploaded by Unravel customers
AWS	Cloud Service Provider	Cloud-based datacenter

People

Unravel has a staff of approximately 100 employees organized in the following functional areas:

- Executive Team (including CEO, finance and legal) - provides overall strategic direction
- Engineering & Quality Assurance (QA) - development team that develops and tests the Unravel Software
- Customer Success - supports customer onboarding, including establishment of account with Unravel and a customer's installation and implementation of the Unravel Software
- Support - provides maintenance/support for customers using the Unravel Software via online portal and ticketing processes
- Sales - develops and nurtures new and existing customer relationships and facilitates sales of Unravel Software and related Support
- IT - manages internal IT systems that support Unravel's business operations

Data

Incident reports are documented in Jira. Alerts are sent out to admins and users via Intercom of any known issues to keep transparent communication with customers. Customer data is stored in accordance with the data protection policy. Unravel software generates and sends log and configuration files to Unravel support on as needed basis to help identify issues with the Unravel software. In addition, Unravel collects data on product usage /analytics (using tools like Matomo, etc., which can be disabled by customers).

Processes, Policies and Procedures

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

Physical Security

Unravel's production instance of the in-scope system and supporting infrastructure is hosted by AWS, GCP, and Azure. As such, AWS, GCP, and Azure are responsible for the physical security controls for Unravel's production instance of the in-scope system. Refer to the "Subservice Organizations" section below for controls managed by the subservice organizations.

Logical Access

Unravel 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, Unravel implements monitoring of one or more of the responsibilities. Monitoring should be performed by a superior without responsibility for performing the conflicting activities or by personnel from a separate department. Resources are managed in the asset inventory system.

Employees sign on to the Unravel network using an Active Directory (AD) user identification (ID) and password. Users are also required to sign on to any systems or applications that do not use the shared sign-on functionality of AD. Passwords are required to conform to defined password standards and are enforced through parameter settings in the AD. 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, requiring reentry of the user ID and password after a period of inactivity.

Customer employees' access Powered Performance Management Software Services System through the Internet using the Secure Sockets Layer (SSL) functionality of their web-browser. These customer employees are required to supply a valid user ID and password to gain access to customer cloud resources. In addition, customers can deploy Unravel on their datacenter servers as well as within their virtual private cloud (VPC) in the cloud. Passwords need to conform to password configuration requirements configured on the virtual devices using the virtual server administration account. Server certificate-based authentication is used as part of the SSL and Transport Layer Security (TLS) encryption with a trusted certificate authority.

Developers accessing the lab and build environment are given access via VPN for remote access by a secure system. Customers can download the Unravel software via a password protected secure connection only.

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

An employee who resigns with notice and who is on good terms with the organization may be permitted to complete projects through his/her separation date. If at any time, the company has reason to suspect that any of its security, property and proprietary information may be compromised as a result of the employee's separation of employment, the company reserves the right to expedite the employee's last day of employment. Within one business day of termination, management shall revoke employee's access to company resources.

On an annual basis, access rules for each role are reviewed by a working group composed of security help desk, data center, customer service, and HR personnel. In evaluating role access, group members consider job description, duties requiring segregation, and risks associated with access. Managers review roles assigned to their direct reports and indicate the required changes in the event management record. The record is routed back to the security team for processing.

Computer Operations - Backups

Unravel software is delivered as a packaged solution that is deployed in the customer environment by the customer. Customers are responsible for managing and maintaining a Backup and Disaster Recovery Policy for the Unravel instance being used. Unravel provides best practices around Backup and Disaster Recovery as part of their documentation. For Software/Systems that are being used within Unravel, there is a defined Backup and Disaster Recovery Policy guide posted in the Google Drive. In the event of an exception, operations personnel perform troubleshooting to identify the root cause.

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to IT 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.

Incident response policies are in place to guide employees on how to report and respond to IT incidents of each type: global, continent, and business. Incident severity is defined by high, medium, and low and the policy for internal employees is for staff to report any incidents or suspected incidents immediately by contacting the person in charge.

Suspected security events are to be reported immediately to the IT support team. If the incident is in relation to paper or hard copy information, for example personal information files that may have been stolen from a filing cabinet need to be reported to the HR Support team above.

Change Control

Unravel maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, QA 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. QA 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. Unravel has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches.

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 Internet protocol (IP) addresses. Administrative access to the firewall is restricted to authorized employees. An IPS is utilized to analyze network events and report possible or actual network security breaches.

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 Unravel. 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 by a third-party vendor on a quarterly basis in accordance with Unravel policy. The third-party vendor uses industry standard scanning technologies and a formal methodology specified by Unravel. 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 Unravel system are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Authorized employees may access the system through from the Internet through the use of leading VPN technology. Employees are authenticated through the use of a token-based multifactor authentication (MFA) system.

Boundaries of the System

The scope of this report includes the Powered Performance Management Software Services System performed in the Palo Alto, California, and Bangalore, India facilities.

This report does not include the cloud hosting services provided by AWS, GCP, and Azure at multiple facilities across the United States and India.

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 Unravel's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Unravel's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

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

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

Commitment to Competence

Unravel'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.

Management considers competence to be what is required to get the job done correctly and on time for each position. Training is provided to every department to increase competence and proper measures are set in place to improve competence over time.

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

Unravel'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.

Management meets in weekly scrums with every department and holds monthly company meetings to cover product and sales to make sure the team is on the same page of company news. Management regularly reviews internal policies and lets employees determine their work schedule during the remote work environment provided at Unravel.

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

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

Organizational Structure and Assignment of Authority and Responsibility

Unravel'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.

Unravel'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. Organizational charts are in place to communicate key areas of authority and responsibility. These charts are communicated to employees and updated as needed.

Human Resources Policies and Practices

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

- Background checks for United States and India employees
- New employees are required to sign acknowledgement forms for the employee handbook
- Supporting evaluations for each employee are performed on a quarterly basis, final evaluations are completed annually
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist

Risk Assessment Process

Unravel's risk assessment process identifies and manages risks to identify significant risks inherent in products or services as they oversee their areas of responsibility. Unravel implements appropriate measures to monitor and manage the risks. This process has identified risks 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 (to make sure the entity is legally and data compliant with the customers)

Unravel's executive team and development teams are responsible for identifying organizational risk and strategic risk assessments on an ongoing basis.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Unravel's Powered Performance Management Software Services System; as well as the nature of the components of the system result in risks that the criteria will not be met. Unravel 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, Unravel'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 Unravel'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, IT. At Unravel, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. General updates to entity-wide security policies and procedures are usually communicated to the appropriate Unravel personnel via e-mail messages.

Specific information systems used to support Unravel's Powered Performance Management Software Services System are described in the Description of Services section above.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Unravel'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

Unravel's management conducts QA 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 Unravel'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 Unravel's personnel.

Reporting Deficiencies

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

Changes to the System Since the Last Review

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

Incidents Since the Last Review

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

Criteria Not Applicable to the System

All Common/Security criteria were applicable to the Unravel Powered Performance Management Software Services System.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS, GCP, and Azure at multiple facilities across United States and India.

Subservice Description of Services

AWS provides flexible, scalable and secure IT infrastructure to businesses of various sizes around the world. With AWS, customers can deploy solutions on a cloud computing environment that provides compute power, storage, and other application services over the Internet as their business needs demand. AWS affords businesses the flexibility to employ the operating systems, application programs and databases of their choice.

GCP provides cloud hosting services that for building, deploying, and scaling applications, websites, and services. It allows Google's infrastructure and tools to run the applications without having to manage physical hardware.

Azure provides cloud hosting services that allows users to access, manage, and develop applications and services through a network of global data centers.

Complementary Subservice Organization Controls

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

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

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4, CC7.2	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.

Subservice Organization - AWS		
Category	**Criteria**	**Control**
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems (IDS) are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
	CC6.7	Backups of critical AWS system components are monitored for successful replication across multiple Availability Zones.

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

Subservice Organization - GCP		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4, CC7.2	The organization has policies and guidelines that govern how to keep the organization's physical workplaces, facilities, and property safe.
		Data center server floors, network rooms, and security systems are physically isolated from public spaces and/or delivery areas.
		Access to sensitive data center zones requires approval from authorized personnel and is controlled via badge readers, secondary identification mechanisms, and/or physical locks.
		Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of their visit.
		Data center perimeters are defined and secured via physical barriers.
		Access lists to high-security areas in data centers are reviewed on a periodic basis and inappropriate access is removed in a timely manner.
		Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.
		Data centers are continuously staffed and monitored by security personnel through the use of real-time video surveillance and/or alerts generated by security systems.
		Visitors to corporate offices must be authenticated upon arrival and remain with an escort for the duration of their visit.

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

Subservice Organization - Azure		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4, CC7.2	Procedures to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors, have been established.
		Security verification and check-in for personnel requiring temporary access to the interior of the datacenter facility, including tour groups or visitors, are required.
		Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team.
		Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.
		The datacenter facility is monitored 24x7 by security personnel.

Unravel management, along with the subservice organizations, define the scope and responsibility of the controls necessary to meet all the relevant Trust Services Criteria through written contracts, such as service level agreements (SLAs). In addition, Unravel performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing attestation reports over services provided by subservice organizations
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organizations

COMPLEMENTARY USER ENTITY CONTROLS

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

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

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

6. User entities are responsible for providing Unravel with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Unravel of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.
8. User entities are responsible for configuring password settings to the production instance of the Unravel application and supporting infrastructure to meet the entity's password policy.
9. User entities are responsible for user access administration to the production instance of the Unravel application and supporting infrastructure, including periodically review access of their personnel.
10. User entities are responsible for reviewing the user activity log for their respective instance of the Unravel application and supporting infrastructure on a periodic basis to validate that activity performed was appropriate.
11. User entities are responsible for the completeness and accuracy of the data input, processed, and output from the in-scope system.
12. User entities are responsible for change management activities that take place within user entity production environments.

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 Unravel's description of the system. Any applicable Trust Services Criteria that are not addressed by control activities at Unravel 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 Unravel was limited to the Trust Services Criteria, related criteria and control activities specified by the management of Unravel and did not encompass all aspects of Unravel'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
- 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 and the employee handbook.	Inspected the employee handbook, information security policies, and the entity's intranet to determine that core values were communicated from executive management to personnel through policies and the employee handbook.	No exceptions noted.
		An employee handbook is documented to communicate workforce conduct standards and enforcement procedures.	Inspected the employee handbook to determine that an employee handbook and code of conduct were documented to communicate workforce conduct standards and enforcement procedures.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook.	Inspected the signed employee handbook for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook.	No exceptions noted.
		Upon hire, personnel are required to complete a background check.	Inspected the background check policies and procedures and the completed background check for a sample of new hires to determine that upon hire, personnel were required to complete a background check.	No exceptions noted.
		Upon hire, personnel are required to sign a confidentiality agreement.	Inspected the signed confidentiality agreement for a sample of new hires to determine that upon hire, personnel were required to sign a confidentiality agreement.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Personnel are required to acknowledge the employee handbook on an annual basis.	Inspected the signed employee handbook for a sample of current employees to determine that personnel were required to acknowledge the employee handbook on an annual basis.	No exceptions noted.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the completed 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 within the employee handbook to determine that sanction policies, which included probation, suspension, and termination, were in place for employee misconduct.	No exceptions noted.
		Employees, third parties, and customers are directed on how to report unethical behavior in a confidential manner.	Inspected the whistleblower policy within the employee handbook and concern form 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 defines and documents the skills and expertise needed among its members.	Inspected the job description for a sample of executive management members to determine that executive management defined and documented the skills and expertise needed among its members.	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 roles and responsibilities are documented and reviewed annually.	Inspected the job description including revision date for a sample of executive management members to determine that executive management roles and responsibilities were documented and reviewed annually.	No exceptions noted.
		Executive management evaluates the skills and expertise of its members annually.	Inspected the completed performance evaluation form for a sample of executive management members to determine that executive management evaluated the skills and expertise of its members annually.	No exceptions noted.
		Executive management maintains independence from those that operate the key controls within the environment.	Inspected the organizational chart and the completed internal controls matrix to determine that executive management maintained independence from those that operated the key controls within the environment.	No exceptions noted.
		Executive management meets annually with operational management to assess the effectiveness and performance of internal controls within the environment.	Inspected the management meeting minutes to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls within the environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Executive management evaluates the skills and competencies of those that operate the internal controls within the environment annually.	Inspected the completed evaluation form for a sample of current employees to determine that executive management evaluated the skills and competencies of those that operate the internal controls within the environment annually.	No exceptions noted.
		Operational management assigns responsibility for and monitors the effectiveness and performance of internal controls implemented within the environment.	Inspected the completed internal controls matrix and management meeting minutes to determine that operational management assigned responsibility for and monitored the effectiveness and performance of internal controls within the environment.	No exceptions noted.
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 intranet.	Inspected the job description for a sample of job roles and the entity's intranet to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's intranet.	No exceptions noted.
		Executive management reviews job descriptions annually and makes updates, if necessary.	Inspected the job description including the revision date for a sample of job roles to determine that executive management reviewed job descriptions annually and made updates, if necessary.	No exceptions noted.
		Executive management has established proper segregations of duties for key job functions and roles within the organization.	Inspected the organizational chart, the completed internal controls matrix, and the job description for a sample of job roles to determine that executive management had 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.
		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 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.

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 completed vendor questionnaire for a sample of vendors 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.	Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.	Inspected the HR policy 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 has a recruiting department that is responsible for attracting individuals with competencies and experience that align with the entity's goals and objectives.	Inspected the refining the recruitment process slide deck to determine that the entity had a recruiting department that was responsible for attracting individuals with competencies and experience that aligned with the entity's goals and objectives.	No exceptions noted.
		The entity evaluates the competencies and experience of candidates prior to hiring.	Inspected the resume and interview notes for a sample of new hires to determine that the entity evaluated the competencies and experience of candidates prior to hiring.	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**
		Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring process.	Inspected the job description for a sample of job roles and the resume and interview notes for a sample of new hires to determine that job requirements were documented in the job descriptions and candidates' abilities to meet these requirements were evaluated as part of the hiring process.	No exceptions noted.
		Upon hire, personnel are required to complete a background check.	Inspected the background check policies and procedures and the completed background check for a sample of new hires to determine that upon hire, personnel were required to complete a background check.	No exceptions noted.
		Employees are required to attend continued training annually that relates to their job role and responsibilities.	Inspected the continued professional education (CPE) training tracker to determine that employees were required to attend continued training annually that related to their job role and responsibilities.	No exceptions noted.
			Inspected the information security awareness training completion form for a sample of current employees to determine that employees were required to attend continued training annually that relates to their job role and responsibilities.	No exceptions noted.

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 tracks and monitors compliance with CPE training requirements.	Inspected the CPE training tracker to determine that executive management tracked and monitored compliance with CPE training requirements.	No exceptions noted.
		Executive management has created a training program for its employees.	Inspected the information security awareness training program to determine that executive management had created a training program for its employees.	No exceptions noted.
		Upon hire, personnel are required to complete information security awareness training.	Inspected the information security awareness training completion form and certificate for a sample of new hires to determine that upon hire, personnel were required to complete information security awareness training.	No exceptions noted.
		The entity has implemented a mentor program to develop its personnel.	Inspected the mentor program materials to determine that the entity had implemented a mentor program to develop its personnel.	No exceptions noted.
		As part of the performance evaluation process, the entity rewards its personnel for exceeding expectations as it relates to their job role and responsibilities.	Inspected the HR policy to determine that as part of the performance evaluation process, the entity rewarded its personnel for exceeding expectations as it related to their job role and responsibilities.	No exceptions noted.
		The entity assesses training needs on an annual basis.	Inspected the internal training program assessment to determine that the entity assessed training needs on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		As part of the entity's contingency plan for job roles and assignments important to the operations and performance of controls, the entity cross trains its personnel.	Inspected the training program materials to determine that as part of the entity's contingency plan for job roles and assignments important to the operations and performance of controls, the entity cross trained its personnel.	No exceptions noted.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet.	Inspected the job description for a sample of job roles and the entity's intranet to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's intranet.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook.	Inspected the signed employee handbook for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook.	No exceptions noted.
		Personnel are required to acknowledge the employee handbook on an annual basis.	Inspected the signed employee handbook for a sample of current employees to determine that personnel were required to acknowledge the employee handbook 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 HR policy 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 has established performance measures, including the incentives and rewards for exceeding expectations, as it relates to job roles and responsibilities.	Inspected the HR policy to determine that executive management had established performance measures, including the incentives and rewards for exceeding expectations, as it relates to job roles and responsibilities.	No exceptions noted.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the completed 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.
		As part of the performance evaluation process, the entity rewards its personnel for exceeding expectations and performs disciplinary actions for its employees who do not meet expectations as it relates to their job role and responsibilities.	Inspected the HR policy to determine that as part of the performance evaluation process, the entity rewarded its personnel for exceeding expectations and performed disciplinary actions for its employees who did not meet expectations as it related to their job role and responsibilities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Executive management reviews the job requirements and responsibilities documented within job descriptions annually and makes updates, if necessary.	Inspected the job description including the revision date for a sample of job roles to determine that executive management reviewed the job requirements and responsibilities documented within job descriptions annually and made updates, if necessary.	No exceptions noted.
		Sanction policies, which include probation, suspension, and termination, are in place for employee misconduct.	Inspected the sanction policies within the employee handbook to determine that sanction policies, which included probation, suspension, and termination, were in place for employee misconduct.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Organizational and information security policies and procedures are documented and made available to personnel through the entity's intranet.	Inspected the organizational and information security policies and procedures and the entity's intranet to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's intranet.	No exceptions noted.
		Edit checks are in place to prevent incomplete or incorrect data from being entered into the system.	Inquired of the Senior Manager regarding edit checks to determine that edit checks were in place to prevent incomplete or incorrect data from being entered into the system.	No exceptions noted.
			Observed the Senior Manager inputting information into the in-scope system to determine that edit checks were in place to prevent incomplete or incorrect data from being entered into the system.	No exceptions noted.
			Inspected the system 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.
		Data flow diagrams and process flowcharts are documented and maintained by management to identify the relevant internal and external information sources of the system.	Inspected the data flow diagrams and process flow charts to determine that data flow diagrams and process flowcharts were documented and maintained by management to identify the relevant internal and external information sources of the system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Data entered into the system, processed by the system and output from the system is protected from unauthorized access.	Inspected the file integrity monitoring (FIM) software configurations, IPS configurations, the encryption methods and configurations for data at rest and in transit, VPN authentication configurations to determine that data entered into the system, processed by the system and output from the system was protected from unauthorized access.	No exceptions noted.
		Data entered into the system is reviewed for completeness and accuracy annually.	Inspected the reviewed data assessment report to determine that data entered into the system was reviewed for completeness and accuracy annually.	No exceptions noted.
		Data processed within the system is reviewed for completeness and accuracy annually.	Inspected the reviewed data assessment report to determine that data processed within the system was reviewed for completeness and accuracy annually.	No exceptions noted.
		Data output from the system is reviewed for completeness and accuracy annually.	Inspected the reviewed data assessment report to determine that data output from the system was reviewed for completeness and accuracy annually.	No exceptions noted.
		Data and information critical to the system are assessed annually for relevance and use.	Inspected the private policy to determine that data and information critical to the system were assessed annually for relevance and 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**
		Data is only retained for as long as required to perform the required system functionality, service, or use.	Inquired of the Senior Manager regarding data retention to determine that data was only retained for as long as required to perform the required system functionality, service, or use.	No exceptions noted.
			Inspected the information management policy to determine that data was only retained for as long as required to perform the required system functionality, service, or use.	No exceptions noted.
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Organizational and information security policies and procedures are documented and made available to personnel through the entity's intranet.	Inspected the organizational and information security policies and procedures and the entity's intranet to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's intranet.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet.	Inspected the job description for a sample of job roles and the entity's intranet to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's intranet.	No exceptions noted.
		The entity's policies and procedures, code of conduct and employee handbook are made available to personnel through the entity's intranet.	Inspected the entity's intranet to determine that the entity's policies and procedures, code of conduct and employee handbook were made available to personnel through the entity's intranet.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Upon hire, personnel are required to read and acknowledge the information security policies and procedures.	Inspected the signed information security policies and procedures acknowledgement for a sample of new hires to determine that upon hire, personnel were required to read and acknowledge the information security policies and procedures.	No exceptions noted.
		Upon hire, personnel are required to complete information security awareness training.	Inspected the information security awareness training completion form and certificate 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 read and acknowledge the information security policies and procedures annually.	Inspected the signed information security policies and procedures acknowledgement for a sample of current employees to determine that current employees were required to read and acknowledge the information security policies and procedures annually.	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.
		Management tracks and monitors compliance with information security and awareness training requirements.	Inspected the information security and 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				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Upon hire, personnel are required to acknowledge the employee handbook.	Inspected the signed employee handbook for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook.	No exceptions noted.
		Personnel are required to acknowledge the employee handbook on an annual basis.	Inspected the signed employee handbook for a sample of current employees to determine that personnel were required to acknowledge the employee handbook on an annual basis.	No exceptions noted.
		Executive management meets annually with operational management to discuss the entity's objectives as well as roles and responsibilities.	Inspected the management meeting minutes to determine that executive management met annually with operational management to discuss the entity's objectives as well as roles and responsibilities.	No exceptions noted.
		Employees, third parties, and customers are directed on how to report unethical behavior in a confidential manner.	Inspected the whistleblower policy within the employee handbook and concern form to determine that employees, third parties, and customers were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.
		Changes to job roles and responsibilities are communicated to personnel through the entity's intranet.	Inspected the intranet to determine that changes to job roles and responsibilities were communicated to personnel through the entity's intranet.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Documented escalation procedures for reporting system failures, incidents, concerns, and other complaints are in place and made available to personnel through the entity's intranet.	Inspected the incident response policies and procedures and the entity's intranet to determine that documented escalation procedures for reporting system failures, incidents, concerns, and other complaints were in place and made available to personnel through the entity's intranet.	No exceptions noted.
		The entity's objectives, including changes made to the objectives, are communicated to its personnel through the entity's intranet.	Inspected the entity's intranet to determine that the entity's objectives, including changes made to the objectives, were communicated to its personnel through the entity's intranet.	No exceptions noted.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The entity's third-party agreements delineate the boundaries of the system and describes relevant system components.	Inspected the master third-party agreement to determine that the entity's third-party agreements delineated the boundaries of the system and described relevant system components.	No exceptions noted.
			Inspected the third-party agreement for a sample of vendors to determine that the entity's third-party agreements delineated the boundaries of the system and described relevant system components.	No exceptions noted.
		The entity's third-party agreements communicate the system commitments and requirements of third parties.	Inspected the master third-party agreement to determine that the entity's third-party agreements communicated the system commitments and requirements of third parties.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the third-party agreement for a sample of vendors to determine that the entity's third-party agreements communicated the system commitments and requirements of third parties.	No exceptions noted.
		The entity's third-party agreements outline and communicate the terms, conditions and responsibilities of third parties.	Inspected the master third-party agreement to determine that the entity's third-party agreements outlined and communicated the terms, conditions and responsibilities of third parties.	No exceptions noted.
			Inspected the third-party agreement for a sample of vendors to determine that the entity's third-party agreements outlined and communicated the terms, conditions and responsibilities of third parties.	No exceptions noted.
		Customer commitments, requirements and responsibilities are outlined and communicated through service agreements.	Inspected the master customer agreement to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.	No exceptions noted.
			Inspected the executed agreement for a sample of customers to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Documented escalation procedures for reporting system failures, incidents, concerns, and other complaints are in place and shared with external parties.	Inspected the third-party agreement for a sample of vendors to determine that documented escalation procedures for reporting failures, incidents, concerns, and other complaints were in place and shared with external parties.	No exceptions noted.
		Executive management meets annually with operational management to discuss the results of assessments performed by third parties.	Inspected the management meeting minutes to determine that executive management met annually with operational management to discuss the results of assessments performed by third parties.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The entity establishes organizational strategies and objectives that are used to determine entity structure and performance metrics.	Inspected the organizational chart, the HR policy and the entity's documented objectives and strategies to determine that the entity established organizational strategies and objectives that were used to determine entity structure and performance metrics.	No exceptions noted.
		Executive management has documented objectives that are specific, measurable, attainable, relevant and time-bound (SMART).	Inspected the entity's documented objectives and strategies to determine that executive management had documented objectives that were SMART.	No exceptions noted.
		Executive management identifies and assesses risks that could prevent the entity's objectives from being achieved.	Inspected the risk assessment policies and procedures to determine that executive management identified and assessed risks that could prevent the entity's objectives from being achieved.	No exceptions noted.
			Inspected the completed risk assessment to determine that executive management identified and assessed risks that could prevent the entity's objectives from being achieved.	No exceptions noted.
		Executive management reviews policies, procedures and other control documents for alignment to the entity's objectives on an annual basis.	Inspected the revision history of the entity’s policies and procedures to determine that executive management reviewed policies, procedures and other control documents for alignment to the entity's objectives on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the management meeting minutes to determine that executive management reviewed policies, procedures and other control documents for alignment to the entity's objectives on an annual basis.	No exceptions noted.
		Executive management reviews and addresses control failures.	Inspected the management meeting minutes to determine that executive management reviewed and addressed control failures.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of internal control failures to determine that executive management reviewed and addressed control failures.	No exceptions noted.
		Executive management has established key performance indicators for operational controls effectiveness, including the acceptable level of control operation and failure.	Inspected the key performance indicators for operational controls effectiveness to determine that executive management established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	No exceptions noted.
		Responsible parties are defined and assigned to coordinate and monitor compliance and audit activities.	Inspected the organizational chart, job descriptions, and information security policies and procedures to determine that responsible parties were defined and assigned to coordinate and monitor compliance and audit activities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity has defined the desired level of performance and operation in order to achieve the established entity objectives.	Inspected the key performance indicators for operational and internal controls effectiveness to determine that the entity had defined the desired level of performance and operation in order to achieve the established entity objectives.	No exceptions noted.
		Key performance indicators of both the business performance and employee performance are developed in alignment with entity objectives and strategies.	Inspected the HR policy, the entity's documented objectives and strategies and the key performance indicators for business and employee performance 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, budgets, and documented objectives and strategies to determine that business plans and budgets aligned with the entity's strategies and objectives.	No exceptions noted.
		Entity strategies, objectives and budgets are assessed on an annual basis.	Inspected the board meeting minutes and slide deck 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 Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework.	Inspected the entity’s compliance reports to determine that the entity's internal controls framework was based on a recognized COSO framework.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity's internal controls environment takes into consideration affecting laws, regulations, standards, and legislatures.	Inquired of the Senior Manager regarding the internal controls environment to determine that the entity's internal controls environment took into consideration affecting laws, regulations, standards, and legislatures.	No exceptions noted.
			Inspected the completed internal controls matrix and privacy policy to determine that the entity's internal controls environment took into consideration affecting laws, regulations, standards, and legislatures.	No exceptions noted.
		Applicable law, regulation, standard and legislature requirements are identified and integrated into the entity's strategies and objectives.	Inspected the entity's documented objectives and strategies and privacy policy to determine that applicable law, regulation, standard and legislature requirements were identified and integrated into the entity's strategies and objectives.	No exceptions noted.
		The entity undergoes compliance audits annually to show compliance to relevant laws, regulations and standards.	Inspected the independent auditors report to determine that the entity underwent compliance audits annually to show compliance to relevant laws, regulations and standards.	No exceptions noted.
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Documented policies and procedures are in place to guide personnel when performing a risk assessment.	Inspected the risk assessment policies and procedures to determine that documented policies and procedures were in place to guide personnel when performing a risk assessment.	No exceptions noted.

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

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

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

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the completed risk assessment to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.
		For gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, are assigned to process owners based on roles and responsibilities.	Inspected the risk assessment policies and procedures 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.
			Inspected the completed risk assessment to determine that for gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, were assigned to process owners based on roles and responsibilities.	No exceptions noted.
		The annual comprehensive risk assessment results are reviewed and approved by appropriate levels of management.	Inspected the risk assessment policies and procedures to determine that the annual comprehensive risk assessment results were reviewed and approved by appropriate levels of management.	No exceptions noted.

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

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

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

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software settings, the FIM software configurations, IPS configurations, and the firewall ruleset for a sample of production servers 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 revision history of the entity's policies and procedures to determine that management reviewed policies, procedures and other control documents for accuracy and applicability on an annual basis.	No exceptions noted.
			Inspected the 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.
		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 management meeting minutes to determine that on an annual basis, management reviewed the controls implemented within the environment for compliance and operational effectiveness and identified potential control gaps and weaknesses.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Logical access reviews are performed quarterly.	Inquired of the Senior Manager regarding user access reviews to determine that logical access reviews were performed quarterly.	No exceptions noted.
			Inspected the completed access review for the in-scope systems for a sample of quarters to determine that logical access reviews were performed quarterly.	No exceptions noted.
		A data backup restoration test is performed on a weekly basis.	Inquired of the Senior Manager regarding restoration testing to determine that a data backup restoration test was performed on a weekly basis.	No exceptions noted.
			Inspected the completed backup restoration test for a sample of weeks to determine that a data backup restoration test was performed on a weekly basis.	No exceptions noted.
		Internal and external vulnerability scans are performed quarterly, and remedial actions are taken where necessary.	Inspected the completed vulnerability scan result for a sample of quarters to determine that internal and external vulnerability scans were performed quarterly, and remedial actions were taken where necessary.	No exceptions noted.
			Inspected the supporting ticket for a sample of vulnerabilities identified by the vulnerability scans to determine that internal and external vulnerability scans were performed quarterly, 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 test annually to identify and exploit vulnerabilities identified within the environment.	Inspected the completed penetration test report to determine that a third party performed a penetration test annually to identify and exploit vulnerabilities identified within the environment.	No exceptions noted.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the completed 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.
		Management obtains and reviews attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third party's environment.	Inspected the completed third-party attestation report and management's review for a sample of vendors to determine that management obtained and reviewed attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third party's environment.	No exceptions noted.
		A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Senior management assesses the results of the compliance, control and risk assessments performed on the environment.	Inspected the management meeting minutes 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 control failures/gaps identified as part of the compliance, control and risk assessments performed.	Inspected the management meeting minutes to determine that senior management was made aware of high-risk vulnerabilities, deviations and controls gaps identified as part of the compliance, control and risk assessments performed.	No exceptions noted.
		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, independent auditors report, completed vulnerability scan results, completed penetration test report performed on the environment 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.

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 incident ticket for a sample of vulnerabilities identified from a vulnerability scan or penetration test to determine that vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment were communicated to those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of deviations identified from the tool used to monitor key systems, tools and applications for compliance 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 incident ticket for a sample of control failures/gaps identified from the internal audit/compliance 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.

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 documented, investigated, and addressed.	Inspected the completed risk assessment, independent auditors report, completed vulnerability scan results, completed penetration test report performed on the environment 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.
			Inspected the supporting incident ticket for a sample of vulnerabilities identified from a vulnerability scan or penetration test to determine that vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment were documented, investigated, and addressed.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of deviations identified from the tool used to monitor key systems, tools and applications for compliance 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 incident ticket for a sample of control failures/gaps identified from the internal audit/compliance 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.
		Vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment are addressed by those parties responsible for taking corrective actions.	Inspected the completed risk assessment, independent auditors report, completed vulnerability scan results, completed penetration test report performed on the environment to determine that vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment were addressed by those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of vulnerabilities identified from a vulnerability scan or penetration test to determine that vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment were addressed by those parties responsible for taking corrective actions.	No exceptions noted.

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 incident ticket for a sample of deviations identified from the tool used to monitor key systems, tools and applications for compliance to determine that vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment were addressed by those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of control failures/gaps identified from the internal audit/compliance assessment to determine that vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment were addressed by those parties responsible for taking corrective actions.	No exceptions noted.
		Management tracks whether vulnerabilities, deviations and control failures/gaps identified as part of the evaluations performed are addressed in a timely manner.	Inspected the management meeting minutes to determine that management tracked whether vulnerabilities, deviations and control failures/gaps identified as part of the evaluations performed were addressed in a timely manner.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	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 and the completed internal controls matrix 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 failures/gaps identified as part of the various evaluations performed.	Inspected the completed risk assessment, completed vulnerability scan results, completed penetration test report performed on the environment to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control failures/gaps identified as part of the various evaluations performed.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of vulnerabilities identified from a vulnerability scan or penetration test to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control failures/gaps identified as part of the various evaluations performed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting incident ticket for a sample of deviations identified from the tool used to monitor key systems, tools and applications for compliance to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control failures/gaps identified as part of the various evaluations performed.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of control failures/gaps to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control failures/gaps identified as part of the various evaluations performed.	No exceptions noted.
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Inspected the organizational chart and the completed internal controls matrix to determine that performance of the internal controls implemented within the environment were assigned to appropriate process owners and operational personnel based on roles and responsibilities.	No exceptions noted.

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**
		Prior to the development and implementation of internal controls into the environment, management considers the complexity, nature, and scope of its operations.	Inquired of the Senior Manager regarding the internal controls environment to determine that prior to the development and implementation of internal controls into the environment, management considered the complexity, nature and scope of its operations.	No exceptions noted.
			Inspected the completed internal controls matrix to determine that prior to the development and implementation of internal controls into the environment, management considered the complexity, nature and scope of its operations.	No exceptions noted.
			Inspected the management meeting minutes to determine that prior to the development and implementation of internal controls into the environment, management considered the complexity, nature and scope of its operations.	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 had documented the relevant controls in place for each key business or operational process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	Inspected the completed internal controls matrix to determine that management had incorporated a variety of controls into their environment that included manual, automated, preventive, detective, and corrective controls.	No exceptions noted.
		Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	Inspected the risk assessment policies and procedures to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
			Inspected the completed risk assessment and the completed internal controls matrix to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of control failures/gaps to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the business continuity and disaster recovery plans, including revision history 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 plan test results to determine that business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.
		An analysis of incompatible operational duties is performed on an annual basis, and where incompatible responsibilities are identified, compensating controls are put into place.	Inspected the organizational chart and the completed internal controls matrix to determine that an analysis of incompatible operational duties was performed on an annual basis, and where incompatible responsibilities were identified, compensating controls were put into place.	No exceptions noted.
			Inspected the supporting communication for reviewing operational duties to determine that an analysis of incompatible operational duties was performed on an annual basis, and where incompatible responsibilities were identified, compensating controls were put into place.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Management has documented the relationship and linkage between business processes, the relevant technologies used to support the business processes, and the controls in place to help secure those business processes.	Inspected the 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.
		Organizational and information security policies and procedures are documented and made available to personnel through the entity's intranet.	Inspected the organizational and information security policies and procedures and the entity's intranet to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's intranet.	No exceptions noted.
		Management has documented the controls implemented around the entity's technology infrastructure.	Inspected the completed internal controls matrix to determine that management had documented the controls implemented around the entity's technology infrastructure.	No exceptions noted.
		Management has established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.	Inspected the completed internal controls matrix to determine that management had established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.	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**
		As part of the risk assessment process, the use of technology in business processes is evaluated by management.	Inspected the completed risk assessment to determine that as part of the risk assessment process, the use of technology in business processes was evaluated by management.	No exceptions noted.
		The internal controls implemented around the entity's technology infrastructure include, but are not limited to: • Restricting access rights to authorized users • Authentication of access • Protecting the entity's assets from external threats	Inspected the completed internal controls matrix to determine that the internal controls implemented around the entity's technology infrastructure included, but were not limited to: • Restricting access rights to authorized users • Authentication of access • Protecting the entity's assets from external threats	No exceptions noted.
		Management has established controls around the acquisition, development and maintenance of the entity's technology infrastructure.	Inspected the completed internal controls matrix to determine that management had established controls around the acquisition, development and maintenance of the entity's technology infrastructure.	No exceptions noted.
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Organizational and information security policies and procedures are documented and made available to personnel through the entity's intranet.	Inspected the organizational and information security policies and procedures and the entity's intranet to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's intranet.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		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 had 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.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet.	Inspected the job description for a sample of job roles and the entity's intranet to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's intranet.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
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 the completed internal controls matrix to determine that performance of the internal controls implemented within the environment were assigned to appropriate process owners and operational personnel based on roles and responsibilities.	No exceptions noted.
		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 the completed internal controls matrix to determine that process owners and management investigated and troubleshot control failures.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of control failures/gaps to determine that process owners and management investigated and troubleshot control failures.	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**
		Effectiveness of the internal controls implemented within the environment are evaluated annually.	Inspected the management meeting minutes to determine that effectiveness of the internal controls implemented within the environment were 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.	Documented policies and procedures are in place regarding system configurations, authentication, access, and security monitoring.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system configurations, authentication, access, and security monitoring.	No exceptions noted.
		An inventory of system assets and components is maintained to classify and manage the information assets.	Inspected the inventory listing of system assets and components to determine that an inventory of system assets and components was maintained to classify and manage the information assets.	No exceptions noted.
	Internal Network - Google Workspace			
		Google Workspace user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Senior Manager regarding Google Workspace access to determine that Google Workspace user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
			Inspected the Google Workspace user listing and access roles to determine that Google Workspace user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Google Workspace administrative access is restricted to authorized personnel.	Inquired of the Senior Manager regarding administrative access to the Google Workspace to determine that Google Workspace 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 Google Workspace administrator listing and access roles to determine that Google Workspace administrative access was restricted to authorized personnel.	No exceptions noted.
		Google Workspace is configured to enforce password requirements that include: • Password expiration • Password length • Complexity	Inspected the Google Workspace password settings to determine that Google Workspace was configured to enforce password requirements that included: • Password expiration • Password length • Complexity	No exceptions noted.
		Google Workspace users are authenticated via individually assigned user accounts and passwords.	Observed the Senior Manager authenticate into Google Workspace to determine that network users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
			Inspected the Google Workspace user listing and password configurations to determine that network users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Google Workspace account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the Google Workspace account lockout configurations to determine that Google Workspace account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		Google Workspace audit logging configurations are in place that include: • Account management • Logon events • Object access • Policy changes • Privilege use • System events	Inspected the Google Workspace audit logging configurations and an example Google Workspace audit log extract to determine that Google Workspace audit logging configurations were in place that included: • Account management • Logon events • Object access • Policy changes • Privilege use • System events	No exceptions noted.
		Google Workspace audit logs are maintained and available for review when needed.	Inquired of the Senior Manager regarding the Google Workspace audit logs to determine that Google Workspace audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example Google Workspace audit log extract to determine that Google Workspace audit logs were maintained and available for review when needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Production Network - AWS			
		AWS user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Senior Manager regarding AWS access to determine that AWS user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
			Inspected the AWS user listing and access roles to determine that AWS user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		AWS administrative access is restricted to authorized personnel.	Inquired of the Senior Manager regarding production administrative access to the AWS to determine that AWS administrative access was restricted to authorized personnel.	No exceptions noted.
			Inspected the AWS administrator listing and access roles to determine that AWS administrative access was restricted to authorized personnel.	No exceptions noted.
		AWS is configured to enforce password requirements that include: • Password history • Maximum password age • Minimum password age • Password length • Complexity	Inspected the AWS password configurations to determine that production servers were configured to enforce password requirements that included: • Password history • Maximum password age • Minimum password age • Password length • Complexity	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		AWS users are authenticated via individually assigned user accounts and passwords.	Observed the Senior Manager authenticate into AWS determine that AWS users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
			Inspected the AWS user listing and password configurations to determine that AWS users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
		AWS account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the AWS account lockout configurations to determine that AWS account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		AWS audit logging configurations are in place that include object access.	Inspected the AWS audit logging configurations and an example AWS audit log extract to determine that AWS audit logging configurations were in place that included object access.	No exceptions noted.
		AWS audit logs are maintained and available for review when needed.	Inquired of the Senior Manager regarding the AWS audit logs to determine that AWS audit logs were maintained and available for review when needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected an example AWS audit log extract to determine that AWS audit logs were maintained and available for review when needed.	No exceptions noted.
	Production Servers - Windows AD			
		Windows AD user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Senior Manager regarding Windows AD access to determine that Windows AD user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
			Inspected the Windows AD user listing and access roles to determine that Windows AD user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Windows AD administrative access is restricted to authorized personnel.	Inquired of the Senior Manager regarding the administrative access to the Windows AD to determine that Windows AD administrative access was restricted to authorized personnel.	No exceptions noted.
			Inspected the Windows AD administrator listing and access roles to determine that Windows AD administrative access was restricted to authorized personnel.	No exceptions noted.
		Windows AD users are authenticated via individually assigned user accounts and passwords.	Observed the Senior Manager authenticate into Windows AD to determine that Windows AD 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**
			Inspected the Windows AD user listings and password configurations to determine that Windows AD users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
		Windows AD account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the Windows AD account lockout settings to determine that operating system account lockout settings were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		Windows AD audit logging configurations are in place and configured to log system events.	Inspected the Windows AD audit logging configurations and an example Windows AD audit log extract to determine that Windows AD audit logging configurations were in place and configured to log system events.	No exceptions noted.
		Windows AD audit logs are maintained and available for review when needed.	Inquired of the Senior Manager regarding the Windows AD audit logs to determine that Windows AD audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example Windows AD audit log extract to determine that Windows AD audit logs were maintained and available for review when needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Production Databases - AWS and Relational Database Service (RDS)			
		AWS database user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Senior Manager regarding AWS database access to determine that AWS user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
			Inspected the user listing and access roles to determine that AWS database user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		AWS database administrative access is restricted to authorized personnel.	Inquired of the Senior Manager regarding administrative access to the AWS database to determine that AWS database administrative access was restricted to authorized personnel.	No exceptions noted.
			Inspected the AWS database administrator listing and access roles to determine that AWS database 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**
		AWS database is configured to enforce password requirements that include: • Password check username • Password length • Mixed case count • Password policy • Special character count • Complexity	Inspected the password configurations for AWS database to determine that AWS database was configured to enforce password requirements that included: • Password check username • Password length • Mixed case count • Password policy • Special character count • Complexity	No exceptions noted.
		AWS database users are authenticated via individually assigned user accounts and passwords.	Observed the Senior Manager authenticate into the AWS database to determine that AWS database users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
			Inspected the AWS database user listings and password configurations to determine that AWS database users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
		AWS database audit logging configurations are in place to log user activity and system events.	Inspected the AWS database audit logging configurations and an example AWS database audit log extract to determine that AWS database audit logging configurations were in place to log user activity and system events.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		AWS database audit logs are maintained and available for review when needed.	Inquired of the Senior Manager regarding the AWS database audit logs to determine that the AWS database audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example AWS database audit log extract to determine that AWS database audit logs were maintained and available for review when needed.	No exceptions noted.
	Production application - Google Workspace and Windows AD			
		Application user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Senior Manager regarding application access to determine that application user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
			Inspected the application user listing and access roles 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 authorized personnel.	Inquired of the Senior Manager regarding administrative access to the application to determine that application administrative access was restricted to authorized personnel.	No exceptions noted.
			Inspected the application administrator listing and access roles to determine that application administrative access was restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The application is configured to enforce password requirements that include: • MFA • Maximum password age • Minimum password age	Inspected the application password configurations to determine that application was configured to enforce password requirements that included: • MFA • Maximum password age • Minimum password age	No exceptions noted.
		Application users are authenticated via individually assigned user accounts and passwords.	Observed the Senior Manager authenticate into the application to determine that application users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
			Inspected the application user listing and password configurations to determine that application users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
		Application account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the application account lockout configurations to determine that application account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.

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 configurations are in place to log user activity and system events.	Inspected the application audit logging configurations and an example application audit log extract to determine that application audit logging configurations were in place to log user activity and system events.	No exceptions noted.
		Application audit logs are maintained and available for review when needed.	Inquired of the Senior Manager regarding the application audit logs to determine that application audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example application audit log extract to determine that application audit logs were maintained and available for review when needed.	No exceptions noted.
	Remote Access - Cisco Meraki, FortiGate, and OpenVPN			
		VPN user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Senior Manager regarding VPN access to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
			Inspected the VPN user listing to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		The ability to administer VPN access is restricted to authorized personnel.	Inquired of the Senior Manager regarding administrative access to the VPN to determine that the ability to administer VPN 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 VPN administrator listing to determine that the ability to administer VPN access was restricted to authorized personnel.	No exceptions noted.
		VPN users are authenticated via valid AD credentials prior to being granted remote access to the system and invalid login attempts are configured to be logged.	Observed the Senior Manager authenticate into the VPN to determine that VPN users were authenticated via valid AD credentials prior to being granted remote access to the system and invalid login attempts were configured to be logged.	No exceptions noted.
			Inspected the VPN authentication configurations to determine VPN users were authenticated via valid AD credentials prior to being granted remote access to the system and invalid login attempts were configured to be logged.	No exceptions noted.
		The entity's various networks are segmented to keep information and data isolated and restricted to authorized personnel.	Inquired of the Senior Manager regarding the entity's networks to determine that the entity's various networks were segmented to keep information and data isolated and restricted to authorized personnel.	No exceptions noted.
			Inspected the network diagram and an external network, a guest wireless network, virtual local area networks (VLANs), VMware configurations, the cloud environment to determine that the entity's various networks were segmented to keep information and data isolated and restricted to authorized personnel.	No exceptions noted.

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**
		Data coming into the environment is secured and monitored through the use of firewalls and an IPS.	Inspected the IPS configurations, network diagram, and firewall ruleset for a sample of production servers to determine that data coming into the environment was secured and monitored through the use of firewalls and an IPS.	No exceptions noted.
		Server certificate-based authentication is used as part of the SSL and 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 SSL and TLS encryption with a trusted certificate authority.	No exceptions noted.
		Passwords and production data is stored in an encrypted format using software supporting the Advanced Encryption Standard (AES).	Inspected the encryption configurations for data at rest to determine that passwords and production data was stored in an encrypted format using software supporting the AES.	No exceptions noted.
		Encryption keys are protected during generation, storage, use, and destruction.	Inquired of the Senior Manager regarding the encryption keys to determine that encryption keys were required to be protected during generation, storage, use, and destruction.	No exceptions noted.
			Inspected the encryption policies and procedures to determine that encryption keys were required to be protected during generation, storage, use, and destruction.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Logical access reviews are performed quarterly.	Inquired of the Senior Manager regarding user access reviews to determine that logical access reviews were performed quarterly.	No exceptions noted.
			Inspected the completed access review for the in-scope systems for a sample of quarters to determine that logical access reviews were performed quarterly.	No exceptions noted.
		Logical access to systems is approved and granted to personnel as a component of the hiring process.	Inquired of the Senior Manager regarding the hiring process to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
			Inspected the hiring procedures, in-scope user listings, and user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked from personnel as a component of the termination process.	Inquired of the Senior Manager regarding the termination process to determine that logical access to systems was revoked from personnel as a component of the termination process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the termination procedures, in-scope user listings, and user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked from personnel as a component of the termination process.	No exceptions noted.
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 configurations, authentication, access, and security monitoring.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system configurations, authentication, access, and security monitoring.	No exceptions noted.
		Logical access to systems is approved and granted to personnel as a component of the hiring process.	Inquired of the Senior Manager regarding the hiring process to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
			Inspected the hiring procedures, in-scope user listings, and user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked from personnel as a component of the termination process.	Inquired of the Senior Manager regarding the termination process to determine that logical access to systems was revoked from personnel as a component of the termination process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the termination procedures, in-scope user listings, and user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked from personnel as a component of the termination process.	No exceptions noted.
		Privileged access to add, remove, or modify access to user accounts is restricted to authorized personnel.	Inquired of the Senior Manager regarding privileged access to sensitive resources to determine that privileged access to add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.
			Inspected the listing of privileged users to the in-scope systems to determine that privileged access to add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.
		Logical access reviews are performed quarterly.	Inquired of the Senior Manager regarding user access reviews to determine that logical access reviews were performed quarterly.	No exceptions noted.
			Inspected the completed access review for the in-scope systems for a sample of quarters to determine that logical access reviews were performed quarterly.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Documented policies and procedures are in place regarding system configurations, authentication, access, and security monitoring.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system configurations, authentication, access, and security monitoring.	No exceptions noted.
		Logical access to systems is approved and granted to personnel as a component of the hiring process.	Inquired of the Senior Manager regarding the hiring process to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
			Inspected the hiring procedures, in-scope user listings, and user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked from personnel as a component of the termination process.	Inquired of the Senior Manager regarding the termination process to determine that logical access to systems was revoked from personnel as a component of the termination process.	No exceptions noted.
			Inspected the termination procedures, in-scope user listings, and user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked from personnel as a component of the termination process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Privileged access to add, remove, or modify access to user accounts is restricted to authorized personnel.	Inquired of the Senior Manager regarding privileged access to sensitive resources to determine that privileged access to add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.
			Inspected the listing of privileged users to the in-scope systems to determine that privileged access to add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.
		Logical access reviews are performed quarterly.	Inquired of the Senior Manager regarding user access reviews to determine that logical access reviews were performed quarterly.	No exceptions noted.
			Inspected the completed access review for the in-scope systems for a sample of quarters to determine that logical access reviews were performed quarterly.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	This criterion is the responsibility of the subservice organizations. Refer to the "Subservice Organizations" section above for controls managed by the subservice organizations.	Not Applicable.	Not Applicable.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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 information management policy to determine that policies and procedures were in place to guide personnel in data, hardware and software disposal and destruction.	No exceptions noted.
		Data that is no longer required is disposed of and rendered unreadable to meet the entity's objectives.	Inspected the information management policy 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 service ticket for a sample of requests to dispose of data to determine that data that was no longer required was disposed of and rendered unreadable to meet the entity's objectives.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	NAT functionality is utilized to manage internal IP addresses.	Inspected the NAT configurations to determine that NAT functionality was utilized to manage internal IP addresses.	No exceptions noted.
		VPN, SSL, TLS and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations, VPN authentication configurations and digital certificates to determine that VPN, SSL, TLS and other encryption technologies were used for defined points of connectivity.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		VPN users are authenticated via valid AD credentials prior to being granted remote access to the system.	Observed the Senior Manager authenticate into the VPN to determine that VPN users were authenticated via valid AD credentials prior to being granted remote access to the system.	No exceptions noted.
			Inspected the VPN authentication configurations to determine that VPN users were authenticated via valid AD credentials prior to being granted remote access to the system.	No exceptions noted.
		Server certificate-based authentication is used as part of the SSL and 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 SSL and TLS encryption with a trusted certificate authority.	No exceptions noted.
		Transmission of digital output beyond the boundary of the system is encrypted.	Inspected the encryption configurations for data in transit and digital certificates to determine that transmission of digital output beyond the boundary of the system was encrypted.	No exceptions noted.
		VPN user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Senior Manager regarding VPN access to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

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 VPN user listing to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	Observed the Senior Manager authenticate into the VPN to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			Inspected the VPN authentication configurations to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
		Logical access to stored data is restricted to authorized personnel.	Inquired of the Senior Manager regarding access to stored data to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
			Inspected the database user listing and access roles to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.

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 firewall ruleset for a sample of production servers to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the firewall ruleset for a sample of production servers to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		An IPS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected the IPS configurations to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IPS is configured to notify personnel upon intrusion detection.	Inspected the IPS notification configurations and an example alert notification to determine that the IPS was configured to notify personnel upon intrusion detection.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Antivirus software is installed on workstations and servers to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus software configuration for a sample of workstations and servers to determine that antivirus software was installed on workstations and servers to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the antivirus software configuration for a sample of workstations and servers and an example antivirus update log to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	No exceptions noted.
		The antivirus software is configured to scan workstations and servers on a daily basis.	Inspected the antivirus software configuration for a sample of workstations and servers to determine that the antivirus software was configured to scan workstations and servers on a daily basis.	No exceptions noted.
		Data is stored in an encrypted format using software supporting the AES.	Inspected the encryption configurations for data at rest to determine that data was stored in an encrypted format using software supporting the AES.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the removable media policy to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the removable media policy to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Logical access to stored data is restricted to authorized personnel.	Inquired of the Senior Manager regarding access to stored data to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
			Inspected the database user listing and access roles to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
		The ability to access backups is restricted to authorized personnel.	Inquired of the Senior Manager regarding access backups to determine that the ability to access backups was restricted to authorized personnel.	No exceptions noted.
			Inspected the listing of users with the ability to access backups to determine that the ability to access backups was restricted to authorized personnel.	No exceptions noted.
		VPN, SSL, TLS and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations, VPN authentication configurations and digital certificates to determine that VPN, SSL, TLS and other encryption technologies were used for defined points of connectivity.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Server certificate-based authentication is used as part of the SSL and 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 SSL and TLS encryption with a trusted certificate authority.	No exceptions noted.
		Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	Observed the Senior Manager authenticate into the VPN to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			Inspected the VPN authentication configurations to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
			Inspected the firewall ruleset for a sample of production servers to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the firewall ruleset for a sample of production servers to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		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.
		An IPS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected the IPS configurations to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IPS is configured to notify personnel upon intrusion detection.	Inspected the IPS notification configurations and an example alert notification to determine that the IPS was configured to notify personnel upon intrusion detection.	No exceptions noted.
		Data is stored in an encrypted format using software supporting the AES.	Inspected the encryption configurations for data at rest to determine that data was stored in an encrypted format using software supporting the AES.	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**
		Backup data is stored in an encrypted format.	Inspected the encryption configurations for backup data to determine that backup data was stored in an encrypted format.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the removable media policy to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
			Inspected the removable media policy to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
		Mobile devices are protected through the use of secured, encrypted connections.	Inspected the encryption configurations to determine that mobile devices were protected through the use of secured, encrypted connections.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organizations. Refer to the “Subservice Organizations” section above for controls managed by the subservice organizations.	Not Applicable.	Not Applicable.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity’s objectives.	The ability to install applications and software on workstations is restricted to authorized personnel.	Inquired of the Senior Manager regarding the applications and software to determine that the ability to install applications and software on workstations was restricted to authorized personnel.	No exceptions noted.

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 warning notification to determine that a warning notification appeared when an employee attempted to download an application or software.	No exceptions noted.
		The ability to migrate changes into the production environment is restricted to authorized and appropriate users.	Inquired of the Senior Manager regarding the change implementation process to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users.	No exceptions noted.
			Inspected the listing 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.
		FIM software is utilized to help detect unauthorized changes within the production environment.	Inspected the FIM software to determine that FIM software was utilized to help detect unauthorized changes within the production environment.	No exceptions noted.
		The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected the FIM software and an example alert generated from the FIM software to determine that the FIM software 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.
		Antivirus software is installed on workstations and servers to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus software configuration for a sample of workstations and servers to determine that antivirus software was installed on workstations and servers to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the antivirus software configuration for a sample of workstations and servers and an example antivirus update log to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	No exceptions noted.
		The antivirus software is configured to scan workstations and servers on a daily basis.	Inspected the antivirus software configuration for a sample of workstations and servers to determine that the antivirus software was configured to scan workstations and servers on a daily basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Information assets, software, hardware, tools, and applications introduced into the environment are scanned for vulnerabilities and malware prior to implementation into the environment.	Inspected the information system and organizational risk assessment to determine that information assets, software, hardware, tools, and applications introduced into the environment were scanned for vulnerabilities and malware prior to implementation 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**
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Management has defined configuration standards in the information security policies and procedures.	Inspected the system configuration standards to determine that management had defined configuration standards in the information security policies and procedures.	No exceptions noted.
		Policies and procedures are in place regarding the detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected the information security policy, incident response policy, and security logging policy to determine that policies and procedures were in place regarding the detection, logging, and monitoring of unknown or unauthorized components into the environment.	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 settings, the FIM software configurations, the IPS configurations, and the firewall ruleset for a sample of production servers 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.

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 and an example monitoring system alert, the FIM notification configurations and an example alert generated from the FIM software, the IPS notification configurations and an example IPS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.
		An IPS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected the IPS configurations to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IPS is configured to notify personnel upon intrusion detection.	Inspected the IPS notification configurations and an example alert notification to determine that the IPS was configured to notify personnel upon intrusion detection.	No exceptions noted.
		FIM software is utilized to help detect unauthorized changes within the production environment.	Inspected the FIM software to determine that FIM software was utilized to help detect unauthorized changes within the production environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected the FIM software and an example alert generated from the FIM software to determine that the FIM software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the removable media policy to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
			Inspected the removable media policy to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
			Inspected the firewall ruleset for a sample of production servers to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the firewall ruleset for a sample of production servers to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		Internal and external vulnerability scans are performed quarterly, and remedial actions are taken where necessary.	Inspected the completed vulnerability scan result for a sample of quarters to determine that internal and external vulnerability scans were performed quarterly, and remedial actions were taken where necessary.	No exceptions noted.
			Inspected the supporting ticket for a sample of vulnerabilities identified by the vulnerability scans to determine that internal and external vulnerability scans were performed quarterly, and remedial actions were taken where necessary.	No exceptions noted.
		A third party performs a penetration test annually to identify and exploit vulnerabilities identified within the environment.	Inspected the completed penetration test report to determine that a third party performed a penetration test annually to identify and exploit vulnerabilities identified within 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.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident response policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		Policies and procedures are in place regarding the detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected the information security policy, incident response policy, and security logging policy to determine that policies and procedures were in place regarding the detection, logging, and monitoring of unknown or unauthorized components into the environment.	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 settings, the FIM software configurations, the IPS configurations, and the firewall ruleset for a sample of production servers 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.

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 alert generated from the FIM software, an example audit log extract from the IPS and an example IPS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.
		An IPS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected the IPS configurations to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IPS is configured to notify personnel upon intrusion detection.	Inspected the IPS notification configurations and an example alert notification to determine that the IPS was configured to notify personnel upon intrusion detection.	No exceptions noted.
		FIM software is utilized to help detect unauthorized changes within the production environment.	Inspected the FIM software to determine that FIM software was utilized to help detect unauthorized changes within the production environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected the FIM software and an example alert generated from the FIM software to determine that the FIM software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
			Inspected the firewall ruleset for a sample of production servers to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the firewall ruleset for a sample of production servers to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		Antivirus software is installed on workstations and servers to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus software configuration for a sample of workstations and servers to determine that antivirus software was installed on workstations and servers to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the antivirus software configuration for a sample of workstations and servers and an example antivirus update log to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	No exceptions noted.
		The antivirus software is configured to scan workstations and servers on a daily basis.	Inspected the antivirus software configuration for a sample of workstations and servers to determine that the antivirus software was configured to scan workstations and servers on a daily basis.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the removable media policy to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
			Inspected the removable media policy to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Internal Network - Google Workspace			
		Google Workspace account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the Google Workspace account lockout configurations to determine that Google Workspace account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		Google Workspace audit logging configurations are in place that include: • Account management • Logon events • Object access • Policy changes • Privilege use • System events	Inspected the Google Workspace audit logging configurations and an example Google Workspace audit log extract to determine that Google Workspace audit logging configurations were in place that included: • Account management • Logon events • Object access • Policy changes • Privilege use • System events	No exceptions noted.
		Google Workspace audit logs are maintained and available for review when needed.	Inquired of the Senior Manager regarding the Google Workspace audit logs to determine that Google Workspace audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example Google Workspace audit log extract to determine that Google Workspace audit logs were maintained and available for review when needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Production Network - AWS			
		AWS account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the AWS account lockout configurations to determine that AWS account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		AWS audit logging configurations are in place that include object access.	Inspected the AWS audit logging configurations and an example AWS audit log extract to determine that AWS audit logging configurations were in place that included object access.	No exceptions noted.
		AWS audit logs are maintained and available for review when needed.	Inquired of the Senior Manager regarding the AWS audit logs to determine that AWS audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example AWS audit log extract to determine that AWS audit logs were maintained and available for review when needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Production Servers - Windows AD			
		Windows AD account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the Windows AD account lockout settings to determine that operating system account lockout settings were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		Windows AD audit logging configurations are in place and configured to log system events.	Inspected the Windows AD audit logging configurations and an example Windows AD audit log extract to determine that Windows AD audit logging configurations were in place and configured to log system events.	No exceptions noted.
		Windows AD audit logs are maintained and available for review when needed.	Inquired of the Senior Manager regarding the Windows AD audit logs to determine that Windows AD audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example Windows AD audit log extract to determine that Windows AD audit logs were maintained and available for review when needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Production Databases - AWS and RDS			
		AWS database audit logging configurations are in place to log user activity and system events.	Inspected the AWS database audit logging configurations and an example AWS database audit log extract to determine that AWS database audit logging configurations were in place to log user activity and system events.	No exceptions noted.
		AWS database audit logs are maintained and available for review when needed.	Inquired of the Senior Manager regarding the AWS database audit logs to determine that the AWS database audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example AWS database audit log extract to determine that AWS database audit logs were maintained and available for review when needed.	No exceptions noted.
	Production application - Google Workspace and Windows AD			
		Application account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the application account lockout configurations to determine that application account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.

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 logging configurations are in place to log user activity and system events.	Inspected the application audit logging configurations and an example application audit log extract to determine that application audit logging configurations were in place to log user activity and system events.	No exceptions noted.
		Application audit logs are maintained and available for review when needed.	Inquired of the Senior Manager regarding the application audit logs to determine that application audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example application audit log extract to determine that application audit logs were maintained and available for review when needed.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organizations. Refer to the “Subservice Organizations” section above for controls managed by the subservice organizations.	Not Applicable.	Not Applicable.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident response policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.

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

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.	Inquired of the Senior Manager regarding incident response policies and procedures to determine that resolution of incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that resolution of incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that resolution of incidents were documented within the ticket and communicated to affected users.	Testing of the control activity disclosed that there were no incidents during the review period.
		A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.	Inquired of the Senior Manager regarding incident response policies and procedures to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the security incident analysis for a sample of critical security incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	Testing of the control activity disclosed that there were no critical security incidents during the review period.
		Incidents resulting in the unauthorized use or disclosure of personal information are communicated to the affected users.	Inquired of the Senior Manager regarding incident response policies and procedures to determine that incidents resulting in the unauthorized use or disclosure of personal information were communicated to the affected users.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that incidents resulting in the unauthorized use or disclosure of personal information were communicated to the affected users.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of critical security incidents that resulted in the unauthorized disclosure of personal information to determine that incidents resulting in the unauthorized use or disclosure of personal information were communicated to the affected users.	Testing of the control activity disclosed that there were no critical security incidents during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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.	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.
		Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident response policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inquired of the Senior Manager regarding incident response policies and procedures to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting incident ticket for a sample of incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Testing of the control activity disclosed that there were no incidents during the review period.
		The actions taken to address identified security incidents are documented and communicated to affected parties.	Inquired of the Senior Manager regarding incident response policies and procedures to determine that the actions taken to address identified security incidents were documented and communicated to affected parties.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that the actions taken to address identified security incidents were documented and communicated to affected parties.	No exceptions noted.
			Inspected the 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.	Testing of the control activity disclosed that there were no incidents during the review period.
		Critical security incidents that result in a service/business operation disruption are communicated to those affected through creation of an incident ticket.	Inquired of the Senior Manager regarding incident response policies and procedures to determine that critical security incidents that result in a service/business operation disruption were communicated to those affected through creation of an incident ticket.	No exceptions noted.

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

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the incident response policies and procedures to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	No exceptions noted.
			Inspected the security incident analysis for a sample of critical security incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	Testing of the control activity disclosed that there were no critical security incidents during the review period.
		The risks associated with identified vulnerabilities are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the supporting incident ticket for a sample of vulnerabilities identified from a vulnerability scan or penetration test to determine that the risks associated with the identified vulnerability were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	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 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.
		Management reviews reports on an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes.	Inspected the management meeting minutes and incident response policy 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.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Change management requests are opened for incidents that require permanent fixes.	Inspected the change management policies and procedures to determine that change management requests were required to be opened for incidents that required permanent fixes.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting change ticket for a sample 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.
		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, backup, 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 infrastructure and operations management policy to determine that data backup and restore procedures were in place to guide personnel in performing backup activities.	No exceptions noted.
		A data backup restoration test is performed on a weekly basis.	Inquired of the Senior Manager regarding restoration testing to determine that a data backup restoration test was performed on a weekly basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the completed backup restoration test for a sample of weeks to determine that a data backup restoration test was performed on a weekly 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 management meeting minutes and incident response policy to determine that management reviewed reports on an annual basis, summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identified the need for system changes and implementation of additional controls based on incident patterns and root causes.	No exceptions noted.
		A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.	Inquired of the Senior Manager regarding incident response policies and procedures to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the security incident analysis for a sample of critical security incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	Testing of the control activity disclosed that there were no critical security incidents during the review period.
		A business continuity and disaster recovery plan are documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	Inspected the business continuity and disaster recovery plans to determine that a business continuity and disaster recovery plan were documented to identify and reduce risks, limited the consequences of damaging incidents, and ensured the timely resumption of essential operations.	No exceptions noted.
		The business continuity and disaster recovery plan are tested on an annual basis.	Inspected the completed business continuity and disaster recovery plan test results to determine that the business continuity and disaster recovery plan were tested on an annual basis.	No exceptions noted.
		The business continuity and disaster recovery plan are updated based on business continuity and disaster recovery plan test results.	Inspected the business continuity and disaster recovery plans, including revision history, and the completed business continuity and disaster recovery test results to determine that the business continuity and disaster recovery plan were updated based on business continuity and disaster recovery plan test results.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Documented change control policies and procedures are in place to guide personnel in the change management process.	Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in the change management process.	No exceptions noted.
		The change management process has defined the following roles and assignments: • Authorization of change requests - Change owner • Development - Change Development team • Testing - QA team • Implementation - Change Coordinator	Inspected the change management policies and procedures to determine that the change management process defined the following roles and assignments: • Authorization of change requests - Change owner • Development - Change Development team • Testing - QA team • Implementation - Change Coordinator	No exceptions noted.
		System changes are communicated to both affected internal and external users.	Inspected the supporting change ticket for a sample of system changes to determine that system changes were communicated to both affected internal and external users.	No exceptions noted.
		The ability to migrate/merge changes into the production environment is restricted to authorized and appropriate users.	Inquired of the Senior Manager regarding the change implementation process to determine that the ability to migrate/merge changes into the production environment was restricted to authorized and appropriate users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the listing of users with the ability to migrate/merge changes into the production environment to determine that the ability to migrate/merge changes into the production environment was restricted to authorized and appropriate users.	No exceptions noted.
		System changes are authorized and approved by management prior to implementation.	Inspected the supporting change ticket for a sample of infrastructure, operating system, database and application 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 version control software and 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.
		Development and test environments are physically and logically separated from the production environment.	Inspected the separate development, test and production environments to determine that development and test environments were physically and logically separated from the production environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		System change requests are documented and tracked in a ticketing system.	Inspected the supporting change ticket for a sample of infrastructure, operating system, database and application changes to determine that system change requests were documented and tracked in a ticketing system.	No exceptions noted.
		A code/peer review is systematically required prior to deploying the Pull Request (PR) into the production environment.	Inspected the supporting change ticket for a sample of infrastructure, database 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.
		FIM software is utilized to help detect unauthorized changes within the production environment.	Inspected the FIM software to determine that FIM software was utilized to help detect unauthorized changes within the production environment.	No exceptions noted.
		The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected the FIM software and an example alert generated from the FIM software to determine that the FIM software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.
		Back out procedures are documented to allow for rollback of application changes when changes impair system operation.	Inspected the backout/rollback procedures and rollback capabilities to determine that back out procedures were documented to allow for rollback of application changes when changes impaired system operation.	No exceptions noted.

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 infrastructure, operating system, database and application changes to determine that system changes were tested prior to implementation and that types of testing performed depended on the nature of the change.	No exceptions noted.
		System changes implemented for remediating incidents follow the standard change management process.	Inquired of the Senior Manager regarding 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 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 incidents to determine that system changes implemented for remediating incidents followed the standard change management process.	Testing of the control activity disclosed that there were no incidents during the review period.
		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.

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 are performed on a configured schedule.	Inspected the system patching configurations and an example patch log for a sample of days to determine that system patches/security updates were performed on a configured schedule.	No exceptions noted.
		Information security policies and procedures document the baseline requirements for the 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 the 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.	Documented policies and procedures are in place to guide personnel in performing risk mitigation activities.	Inspected the risk assessment policies and procedures to determine that documented policies and procedures were in place to guide personnel in performing risk mitigation activities.	No exceptions noted.
		Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	Inspected the risk assessment policies and procedures to determine that management had defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	No exceptions noted.
		A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.
		Identified risks are rated using a risk evaluation process and ratings are approved by management.	Inspected the risk assessment policies and procedures 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**
			Inspected the completed risk assessment to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
		Risks identified as a part of the risk assessment process are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the risk assessment policies and procedures 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.
			Inspected the completed risk assessment to determine that risks identified as a part of the risk assessment process were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the risk assessment policies and procedures to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.

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

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management obtains and reviews attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third party's environment.	Inspected the completed third-party attestation report and management's review for a sample of vendors to determine that management obtained and reviewed attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third party's environment.	No exceptions noted.
		A 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 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.
			Inspected the completed vendor questionnaire for a sample of vendors 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 has assigned responsibility and accountability for the management of risks associated with third parties to appropriate personnel.	Inspected the organizational chart, job descriptions, and vendor management policies and procedures to determine that management had 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 vendor management policies and procedures to determine that management had 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 vendor management policies and procedures to determine that the entity had documented procedures for addressing issues identified with third parties.	No exceptions noted.
		The entity has documented procedures for terminating third-party relationships.	Inspected the vendor management policies and procedures to determine that the entity had documented procedures for terminating third-party relationships.	No exceptions noted.