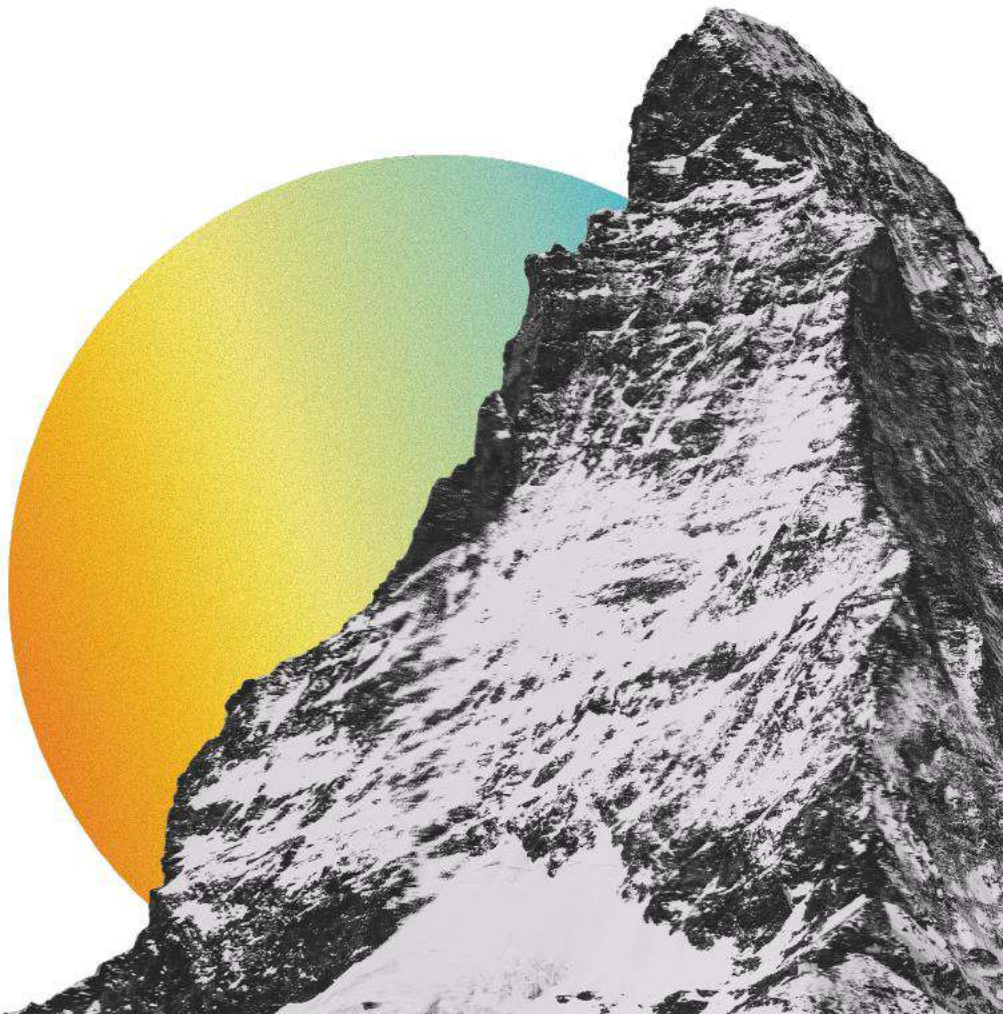
A-LIGN

Mango Practice, Inc.

Type 2 SOC 2

2024



REPORT ON MANGO PRACTICE, INC.'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

September 1, 2024 to November 30, 2024

Table of Contents

SECTION 1

ASSERTION OF MANGO PRACTICE, INC. MANAGEMENT

ASSERTION OF MANGO PRACTICE, INC. MANAGEMENT

December 10, 2024

We have prepared the accompanying description of Mango Practice, Inc.'s ('Mango' or 'the Company') Management Software Services titled "Mango Practice, Inc.'s Description of Its Management Software Services throughout the period September 1, 2024 to November 30, 2024" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the Management Software Services that may be useful when assessing the risks arising from interactions with Mango's system, particularly information about system controls that Mango 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*).

Mango uses Amazon Web Services ('AWS') and Google Cloud Platform ('GCP') 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 Mango, to achieve Mango's service commitments and system requirements based on the applicable trust services criteria. The description presents Mango's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Mango'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 Mango, to achieve Mango's service commitments and system requirements based on the applicable trust services criteria. The description presents Mango's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Mango's controls.

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

a. the description presents Mango's Management Software Services that was designed and implemented throughout the period September 1, 2024 to November 30, 2024, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period September 1, 2024 to November 30, 2024, to provide reasonable assurance that Mango'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 Mango's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period September 1, 2024 to November 30, 2024, to provide reasonable assurance that Mango'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 Mango's controls operated effectively throughout that period.

Randall Robinson

Randall Robinson
CFO
Mango Practice, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Mango Practice, Inc.

Scope

We have examined Mango's accompanying description of its Management Software Services titled "Mango Practice, Inc.'s Description of Its Management Software Services throughout the period September 1, 2024 to November 30, 2024" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period September 1, 2024 to November 30, 2024, to provide reasonable assurance that Mango'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*).

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

The information included in Section 5, "Other Information Provided by the Service Organization," is presented by Mango management to provide additional information and is not a part of the description. Information about Mango's management's response to testing exceptions has not been subjected to the procedures applied in the examination of the description, the suitability of the design of controls, and the operating effectiveness of the controls to achieve Mango's service commitments and system requirements based on the applicable trust services criteria.

Service Organization's Responsibilities

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

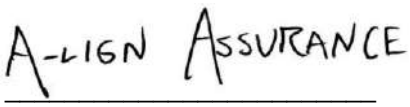
a. the description presents Mango's Management Software Services that was designed and implemented throughout the period September 1, 2024 to November 30, 2024, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period September 1, 2024 to November 30, 2024, to provide reasonable assurance that Mango'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 Mango's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period September 1, 2024 to November 30, 2024, to provide reasonable assurance that Mango'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 Mango'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 Mango, user entities of Mango's Management Software Services during some or all of the period September 1, 2024 to November 30, 2024, business partners of Mango subject to risks arising from interactions with the Management Software Services, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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



Tampa, Florida
December 10, 2024

SECTION 3

MANGO PRACTICE, INC.'S DESCRIPTION OF ITS MANAGEMENT SOFTWARE SERVICES THROUGHOUT THE PERIOD SEPTEMBER 1, 2024 TO NOVEMBER 30, 2024

OVERVIEW OF OPERATIONS

Company Background

Mango Practice Management is a software company that offers practice management solutions tailored primarily for accounting and other professional service firms. Initially founded in 1999 by CPA Fred Lindsley as ImagineTime, ImagineTime's primary product was designed to streamline time and billing, improve visibility for accountants, and integrate workflow management. In 2018, new leadership set out to modernize the platform, adding features like secure file sharing (MangoShare) and electronic signatures.

In 2020, ImagineTime merged with Mango Billing to form Mango Practice Management. This rebranding resulted in a comprehensive suite that includes time tracking, billing, client portals, document sharing, and integration with major software like QuickBooks, UltraTax, and Lacerte. Mango Practice Management now serves nearly 2,000 firms, helping them improve productivity and profitability by automating time-consuming tasks like billing and document management.

For firms seeking all-in-one solutions, Mango Practice Management offers a customizable user experience with robust reporting, secure client portals, and time-tracking capabilities that integrate seamlessly into everyday workflow tasks, making it highly adaptable for accounting firms and consultants alike.

Description of Services Provided

Mango Practice Management offers a suite of services aimed at streamlining workflow, billing, and client interactions for accounting firms and other professional services. Key offerings include:

1. **Time and Billing Management:** Allows firms to efficiently track billable hours, manage invoicing, and automate billing processes with customizable billing formats and recurring billing options.
2. **Workflow and Project Management:** This feature helps firms manage deadlines, allocate tasks, and track project progress. It's useful for due date tracking and organizing multiple client engagements efficiently.
3. **Document Management and Secure File Sharing:** Through MangoShare, firms can share documents securely with clients, allowing for safe file exchange and electronic signatures, which simplifies document handling and improves compliance.
4. **Client Portals and Collaboration Tools:** Mango Practice Management provides a client portal, which includes document management, messaging, and collaboration tools, making it easy for clients to communicate with the firm and access shared resources securely.
5. **Analytics and Reporting:** Mango Practice Management's reporting tools provide insights into firm performance, productivity, and client data. The platform includes customizable reporting options and dashboards that help in tracking financial and operational metrics.
6. **Integration Capabilities:** Mango Practice Management integrates with widely used accounting and tax software, including QuickBooks, UltraTax, and Lacerte, allowing seamless data flow between applications used by accountants and their clients.

Mango Practice Management's all-in-one approach makes it a strong choice for firms looking to consolidate essential functions like billing, workflow, and document handling within a single platform.

Principal Service Commitments and System Requirements

Mango Practice Management designs its processes and procedures related to Accounting Practice Management. These objectives are based on service commitments made to clients, applicable laws and regulations governing the provision of Mango Practice services, and Mango's own financial, operational, and compliance requirements. Security commitments to clients are documented in Terms of Service. Standardized security commitments include but are not limited to:

- **Role-Based Access Control:** Security principles are embedded within the design of the TMS, allowing users to access the information needed for their specific role while restricting access to data outside of their role.
- **Encryption:** Customer data is protected through encryption technologies, ensuring data security both at rest and in transit.

Mango Practice Management establishes operational requirements that support its security commitments, comply with relevant laws and regulations, and meet other system requirements. These requirements are communicated through Mango's system policies and procedures, system design documentation, and customer contracts. Information security policies outline an organization-wide approach to protecting systems and data. Policies cover system design and development, operational procedures, management of internal business systems and networks, and employee hiring and training.

In addition to these policies, Mango has documented standard operating procedures (SOPs) that detail specific manual and automated processes essential for the operation and development of the TMS.

Components of the System

Infrastructure

Primary infrastructure used to provide Mango Management Software Services includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Amazon Web Services	Cloud Hosting	Host Mango Practice Management
Google Cloud Platform	Cloud Hosting	Host MangoShare

Software

Primary software used to provide Mango Management Software Services includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Mango Practice Management	Cloud	Accounting Practice Management
MangoShare	Cloud	File sharing and e-signature solution
SalesForce	Cloud	Sales Opportunity & Customer Management System
Jira	Cloud	Software Ticketing System

People

- *Corporate*. Mango Practice Management employs executives and senior operations staff who oversee key functional areas, including corporate administration, compliance, finance, accounting, and legal. This team uses the Mango platform to monitor overall company performance, develop internal metrics, and generate high-level reports that support Mango's service offerings for accounting firms and other clients.
- *Operations*. Operations staff manage the day-to-day service aspects within the Mango platform, ensuring smooth client support, workflow management, and billing functions. These roles include:
    - Client Service Representatives: These representatives handle support queries from Mango's user firms, providing assistance for billing, time tracking, and report generation.
    - Workflow Coordinators: Workflow coordinators manage task assignments within the Mango system, overseeing client collaboration tools and monitoring task completion across teams.
    - Quality Assurance Specialists: Responsible for reviewing sample reports and data entries for contractual compliance, quality assurance staff help ensure accuracy and monitor for potential misuse or errors within Mango's system.
- *IT.* The IT department at Mango Practice Management includes personnel dedicated to infrastructure management, networking, information security, and software development. Responsibilities include:
    - Help Desk and Technical Support: This group assists Mango users with technical issues related to system access, data entry, and navigation within the platform.
    - Infrastructure, Networking, and Systems Administration: These roles provide foundational support, ensuring the Mango Practice Management software is secure and operational. They manage system updates and release new software versions into the live environment.
    - Software Development and Quality Assurance: Mango's development team maintains the platform, adding features and ensuring system compatibility with integrations like QuickBooks and tax software (e.g., UltraTax, Lacerte). Quality assurance tests these updates for performance and security before public release.
    - Information Security: The security team monitors threats to ensure that client data remains private and secure. They also manage antivirus and network security, conducting regular audits of Mango's IT assets.
- *Procedures*. Mango has standardized procedures for managing system updates, user training, and client support. Regular software updates add features or address vulnerabilities, while the support team assists users with troubleshooting and technical inquiries. All team members follow data protection protocols to ensure compliance and security when handling client data.
- *Data.* Data is integral to Mango's functionality, supporting billing, time tracking, and client interactions. Mango's system ensures secure data storage and provides firms with data-backed insights for workflow improvements. Reports generated from Mango's data provide visibility into client billing, task completion, and other operational metrics.

This structure enables Mango Practice Management to provide an efficient, secure, and user-friendly practice management system for accounting firms and professional service providers.

Data

Files, as defined by Mango Practice Management, constitute the following:

- Accounting file data
- Transaction records
- Electronic interface files related to accounting
- Financial output reports
- Input reports for accounting processes
- Legal documents requiring signatures

Transaction processing is initiated by the receipt of a payment request or standing billing order. This request typically comes directly from a user or facility by email, through a web portal, or via secure HTTP from an external partner. After the transaction is completed, the accounting team receives electronic documents with transaction details, including completed transactions, cancellations, or adjustments, and weekly financial logs. All information is entered into the system's verification module; a portion of this completion information may be entered on the Mango Practice Management accounting provider web interface.

Output reports are available in electronic PDF, comma-separated value file exports, or through the accounting web portal. The availability of these reports is limited by job function. Reports delivered externally are only sent using secure methods-encrypted email, secure HTTP, or secure websites-to authorized providers, auditors, and regulatory agencies. Mango Practice Management uses Transport Layer Security to encrypt email exchanges with government auditors, partner facilities, and external providers.

Processes, Policies and Procedures

Formal IT Policies and Procedures

Mango Practice Management has established formal IT policies and procedures that cover cloud infrastructure security, logical access, system operations, change control, and data communication standards. All teams are expected to follow these policies and procedures, which define the framework for securely delivering services. These documents are available on the Company’s intranet and can be accessed by any Mango team member.

Cloud Infrastructure Security

Mango Practice Management’s cloud-hosted environment is protected by strict access controls and robust security protocols. The cloud infrastructure is hosted in secure data centers managed by the cloud provider, which adheres to industry standards for physical and environmental security, including restricted access areas, biometric authentication, and 24/7 monitoring. Only authorized personnel from the cloud provider have access to the physical data center facilities.

Logical Access Control

Access to Mango's cloud-hosted environment is restricted based on user roles and responsibilities. Authorized team members are granted access to specific applications, data sets, and services through an access control system. Authentication requires multi-factor authentication (MFA), and each user is assigned access rights according to job responsibilities. Users can only access data and systems necessary for their roles, enforced through identity and access management (IAM) policies.

Access to sensitive data within the cloud environment is controlled using security groups and virtual private networks (VPNs), ensuring segmentation and isolation. Network zones are configured within the cloud to control access to critical components, and access is further managed through access control lists (ACLs) and security group rules.

Visitor and Vendor Access

While the cloud environment does not have a traditional reception area, all third-party vendors who require access to Mango's cloud resources undergo a strict approval process. Vendors must present a valid reason for access, and their accounts are provisioned with temporary, limited-access credentials based on the principle of least privilege. Vendor access is logged and monitored, with each session tracked for audit purposes. Vendor accounts automatically expire after a set period, and any extension requires approval from authorized Mango personnel.

Access to Sensitive Resources

Access to high-security resources, such as databases and virtual machines that handle sensitive data, is controlled by multiple layers of authentication. Authorized personnel must first authenticate with a password and then complete a second authentication step using a MFA token within the cloud provider's secure console.

Employee Termination Procedures

When an employee's employment with Mango Practice Management ends, the HR team initiates an access termination request within the access management system on the last day of employment. This request is routed to access administrators for prompt removal of the employee's credentials. Multi-factor authentication devices and tokens assigned to the employee are also collected and deactivated. On a monthly basis, the director of cloud security reviews a report of recently deactivated accounts to confirm that all necessary access removals have been completed.

Quarterly Access Review

Each quarter, the cloud security team generates access reports for key areas within the cloud environment. These reports are distributed to designated zone owners (such as application, database, and network administrators) through the access management system. Zone owners review access records, noting any required changes, and submit the updated access requirements back to access administrators for action. The director of cloud security monitors any outstanding reviews and follows up with zone owners to ensure completion.

Semi-Annual Vendor Access Review

On an annual basis, the Director of Information Security provides each vendor with a list of their personnel who have access to Mango's cloud-hosted environment. Vendors are required to review the list, confirm the appropriateness of each employee's access, and return the confirmation within two weeks. The director follows up with vendors as needed to ensure compliance with access review procedures.

Physical Security

The in-scope system and supporting infrastructure is hosted by AWS and GCP. As such, AWS and GCP is responsible for the physical security controls for the in-scope system. Please refer to the "Subservice Organization" section below for detailed controls.

Logical Access

Mango Practice Management uses a role-based security architecture and requires system users to be identified and authenticated before accessing any resources. Resources are protected using the system's native security features along with additional software that identifies and authenticates users, validating access requests against authorized roles defined in access control lists. If conflicting responsibilities cannot be fully segregated, Mango implements monitoring for one or more of those responsibilities. This monitoring is conducted by a supervisor with no involvement in the conflicting tasks or by personnel from a separate department.

All resources are tracked in the asset inventory system, and each asset has an assigned owner. Asset owners are responsible for approving access to the resource and conducting periodic access reviews based on assigned roles.

Employees and approved vendors log in to the Mango network using an Active Directory user ID and password. Users must separately sign on to any systems or applications that do not use Active Directory's shared sign-on feature. Passwords must comply with defined standards, enforced through Active Directory settings. These settings require users to update their passwords at regular intervals, restrict system access after a set number of unsuccessful login attempts, and lock screens, requiring reentry of the user ID and password after a period of inactivity.

Employees accessing the system from outside the Mango network must use a token-based two-factor authentication system. Tokens are issued upon employment and must be returned during the exit process. Vendor personnel are not permitted to access the system externally.

Customer employees access Mango Practice Management services over the Internet using SSL encryption via their web browser. These users must provide a valid user ID and password to access cloud resources, with passwords required to meet configuration standards set on virtual devices by the virtual server administration account. Virtual devices are initially configured per Mango's standards, although configurations may be modified by the virtual server administration account.

Customer employees may also access their systems using virtual server administration accounts, which require a two-factor authentication system based on digital certificates.

When a new employee is hired, they are assigned a position in the HR management system. With less than a week before their start date, the HR team generates a report listing new user IDs to be created. The employee’s manager makes additional requests for permissions necessary to the employees’ role. This report is used by the security help desk to set up user IDs and access rules, which are predefined based on role requirements. The report also includes employees with position changes, enabling updates to access rules as necessary.

Annually, a working group of personnel from the security help desk, data center, customer service, and HR departments reviews access rules for each role. This review considers job descriptions, segregation of duties, and access-related risks. Completed access rules are then reviewed and approved by the Director of Information Security. During this process, the Director of Information Security reviews privileged roles and requests modifications as needed.

Quarterly, managers review the roles assigned to their direct reports. Security generates and distributes role lists to managers through the event management system. Managers indicate necessary changes in the event management record, which is then routed to the security help desk for processing. The security help desk manager identifies any records not returned within two weeks and follows up with the manager. As part of this process, the Director of Information Security reviews employees with privileged access and requests modifications as necessary through the event management system.

Computer Operations - Backups

Customer data is backed up and monitored by operations personnel for completion and any exceptions. In the event of an exception, operations personnel troubleshoot to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job, depending on the customer’s specified preference outlined in documented work instructions.

The backup infrastructure is fully cloud-based, with digital backups stored in secure, geographically dispersed cloud data centers. This infrastructure resides on private networks, logically secured and isolated from other networks to ensure data integrity and security.

Computer Operations - Availability

Incident Response Policies and Procedures

Mango Practice Management has established incident response policies and procedures to guide personnel in reporting and responding to information technology incidents. These procedures outline the steps for identifying, reporting, and addressing security breaches and other incidents to ensure a timely and effective response. Incident response processes are specifically designed to identify and respond to network-related incidents within the cloud hosted environment.

Capacity Monitoring and Management

Mango Practice Management continuously monitors the capacity utilization of cloud-based computing resources, ensuring that service delivery aligns with service level agreements. Capacity monitoring is conducted for both internal and customer resources, allowing Mango to proactively evaluate the need for additional infrastructure in response to customer growth or new customer onboarding. Cloud infrastructure capacity monitoring includes, but is not limited to:

- Virtual machine and storage capacity
- Network bandwidth
- Compute resources (e.g., CPU, memory)

This monitoring helps ensure that sufficient resources are available to meet performance and availability requirements as customer needs evolve.

Patch Management Process

Mango Practice Management has implemented a robust patch management process to ensure that customer and infrastructure systems are updated in line with vendor-recommended patches. Proposed patches are reviewed by both Mango system administrators and customer representatives to determine applicability based on each system's security and operational requirements. This review process considers the security and availability impact on critical applications hosted within the cloud environment.

Mango's operations team validates that all approved patches have been installed and that any necessary system reboots have been completed to ensure full implementation. This proactive approach helps maintain a secure and stable infrastructure for all cloud-hosted services.

Change Control

Mango Practice Management maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in planning, documenting, and implementing changes to applications and cloud infrastructure. Change control procedures encompass change request initiation, documentation requirements, development practices, quality assurance testing, and required approval processes.

A ticketing system is used to document the change control procedures for both application updates and the implementation of new infrastructure changes. Quality Assurance (QA) testing and User Acceptance Testing (UAT) results are recorded and maintained within the change request record in the ticketing system. Development and testing occur in environments that are logically separated from the production environment, ensuring a secure and controlled change process. All changes receive management approval before migration to the production environment, and approvals are documented in the ticketing system.

Version control software is used to maintain source code versions and manage the code's progression from development to production. This software keeps a complete history of code changes, supporting rollback capabilities, and tracking changes to individual developers, ensuring accountability and traceability throughout the change process.

Patch Management Process

Mango Practice Management has established a patch management process to ensure that customer systems and internal infrastructure are updated with vendor-recommended patches. Both Mango system administrators and customers review proposed patches to assess their applicability based on the security and availability needs of the systems involved, as well as any critical applications hosted on them.

Mango's operations team verifies that all approved patches have been installed and, if required, that any necessary system reboots have been completed. This approach helps maintain secure, stable, and updated systems across the cloud infrastructure.

Data Communications

Firewall and Network Security

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any network connections that are not explicitly authorized. Network Address Translation (NAT) functionality is used to manage internal IP addresses securely. Administrative access to the firewall is restricted to authorized employees only, ensuring that network configurations are protected against unauthorized changes.

Redundancy is built into the cloud infrastructure supporting Mango Practice Management's services to eliminate single points of failure. This redundancy includes firewalls, routers, and virtualized servers. In the event of a primary system failure, redundant hardware or virtual instances are configured to automatically take over, maintaining continuous service availability.

Penetration Testing

Penetration testing is conducted regularly to evaluate the security posture of Mango's cloud-hosted environment. A third-party vendor, following an industry-standard penetration testing methodology specified by Mango Practice Management, performs these tests. The process begins with a vulnerability analysis of the environment to identify exploitable vulnerabilities, simulating scenarios of internal threats or external attacks. Once vulnerabilities are identified, the vendor attempts to exploit them to assess potential unauthorized access or malicious activity risks. Penetration testing includes both network and application layer testing, as well as evaluating controls and processes surrounding network and application security. Tests are conducted from both external (outside) and internal (inside) perspectives to ensure comprehensive security coverage.

Vulnerability Scanning

A third-party vendor performs vulnerability scanning on a quarterly basis in accordance with Mango's policies. The vendor uses industry-standard scanning technologies, and a formal methodology specified by Mango Practice Management. These scanning tools are configured to thoroughly test the infrastructure and applications while minimizing any risks associated with active scanning. Retests and on-demand scans are conducted as necessary, and scans are scheduled during non-peak times. Any tools requiring installation within Mango's environment are implemented through the Change Management process, ensuring that scanning activities are documented and authorized. Approved scanning templates and bandwidth-throttling options are enabled to ensure efficient scanning without impact on operational performance.

Remote Access Security

Authorized employees may access Mango's systems securely from the Internet using advanced VPN technology. Employees are authenticated through a token-based two-factor authentication system, adding an extra layer of security for remote access.

Boundaries of the System

The scope of this report includes the Management Software Services performed in the Rutherfordton, North Carolina Facilities.

This report does not include the cloud hosting services provided by AWS and GCP at multiple facilities.

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

Control Environment

Integrity and Ethical Values

The effectiveness of controls is inherently linked to the integrity and ethical values of the individuals who design, implement, and monitor these controls. Integrity and ethical values form the foundation of Mango Practice Management's control environment, influencing the design, administration, and oversight of all control components. Mango's commitment to integrity and ethical behavior is reflected in its ethical and behavioral standards, how these standards are communicated, and how they are reinforced through organizational practices. This commitment includes management's efforts to mitigate incentives or pressures that could lead personnel to engage in dishonest, illegal, or unethical acts. Additionally, it encompasses the communication of organizational values and behavioral expectations to all employees through policy statements, codes of conduct, and leading by example.

Specific control activities that Mango Practice Management has implemented in this area are outlined below:

- **Organizational Policy Statements and Codes of Conduct:** Mango communicates its core values and behavioral standards to employees through formally documented policies and codes of conduct.
- **Acknowledgment of Policies and Procedures:** Employees are required to sign an acknowledgment form confirming they have received access to the employee manual and understand their obligation to comply with the policies and procedures outlined in it.
- **Confidentiality Agreement:** The employee handbook includes a confidentiality statement, where employees agree not to disclose proprietary or confidential information, including client information, to unauthorized individuals.
- **Background Checks:** As part of the hiring process, Mango conducts background checks for all employees to ensure a safe and trustworthy workforce.

Commitment to Competence

Mango Practice Management's leadership defines competence as the knowledge and skills essential for employees to effectively fulfill their roles and responsibilities. Management's commitment to competence includes assessing the competence levels required for specific roles and ensuring these translate into the necessary skills and knowledge for successful job performance.

Specific control activities that Mango Practice Management has implemented in this area are outlined below:

- **Defined Competency Requirements:** Management has evaluated the required competence levels for specific roles and documented these as part of written job requirements, specifying the skills and knowledge necessary for each position.
- **Ongoing Training:** Training is provided to personnel in certain roles to maintain and enhance their skill levels, ensuring continued competence in key positions.

Management's Philosophy and Operating Style

Mango Practice Management's management philosophy and operating style encompass a variety of characteristics, including its approach to assessing and managing business risks, and its attitudes toward information processing, accounting functions, and personnel management.

Specific control activities that Mango Practice Management has implemented in this area include:

- **Regulatory and Industry Updates:** Management is periodically briefed on regulatory and industry changes that impact the services provided, ensuring alignment with compliance and best practices.
- **Executive Management Meetings:** Executive management holds regular meetings to discuss major initiatives and key issues that influence the business as a whole, fostering informed decision-making and strategic oversight.

Organizational Structure and Assignment of Authority and Responsibility

Mango Practice Management's organizational structure provides the framework within which activities for achieving company-wide objectives are planned, executed, controlled, and monitored. Management believes that establishing an effective organizational structure involves considering key areas of authority and responsibility. The organizational structure has been designed to suit the company's needs, taking into account its size and the nature of its operations.

Mango's assignment of authority and responsibility includes determining how authority and responsibility for operational activities are assigned, along with establishing reporting relationships and authorization hierarchies. This includes policies regarding business practices, the knowledge and experience of key personnel, and the resources provided to fulfill their duties. Additionally, it involves policies and communications aimed at ensuring personnel understand the organization's objectives, know how their roles contribute to these objectives, and understand their responsibilities and accountabilities.

Specific control activities that Mango Practice Management has implemented in this area include:

- **Organizational Charts:** Each Job has an associated Job Description detailing roles, responsibilities and reporting structure.
- **Regular Updates and Communication:** Organizational charts are communicated to employees and updated as needed to reflect changes in roles and responsibilities.

Human Resource Policies and Practices

Mango Practice Management's success is built on a foundation of strong business ethics, reinforced by a high level of efficiency, integrity, and ethical standards. This commitment has resulted in a proven track record of hiring and retaining top-quality personnel, ensuring that the organization operates at maximum efficiency. Mango's human resources policies and practices encompass employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary actions.

Specific control activities that Mango Practice Management has implemented in this area include:

- **Employee Handbook Acknowledgment:** New employees are required to sign acknowledgment forms for the employee handbook and a confidentiality agreement as part of the new hire orientation on their first day of employment.
- **Annual Evaluations:** Employee performance evaluations are conducted on an annual basis to support professional development and ensure alignment with organizational goals.
- **Employee Termination Procedures:** Documented employee termination procedures guide the termination process, supported by a comprehensive termination checklist to ensure consistency and compliance.

Risk Assessment Process

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

Through this process, Mango has identified key risks related to the nature of its services and has implemented various strategies to address these risks. Identified risks include:

- **Operational Risk** - Changes in the environment, staff, or management personnel
- **Strategic Risk** - Emerging technologies, evolving business models, and industry shifts
- **Compliance Risk** - Legal and regulatory changes

Mango Practice Management has also established an independent business unit responsible for identifying organizational risks and monitoring the effectiveness of internal controls. This unit's approach aims to align the organization's strategy more closely with key stakeholders, assist teams in managing uncertainty, minimize potential threats, and capitalize on opportunities in a rapidly changing market.

Mango actively identifies and mitigates significant risks through ongoing initiatives and continuous communication with other leadership teams and senior management.

Integration with Risk Assessment

The environment in which Mango Practice Management's Practice Management system operates, along with the commitments, agreements, and responsibilities associated with the system, creates unique risks that the criteria may not be met. Mango addresses these risks through the implementation of appropriately designed controls to provide reasonable assurance that the criteria are achieved. Given that each system and its operating environment are unique, the combination of risks to meeting the criteria and the controls needed to mitigate those risks will also be unique.

As part of the system's design and operation, Mango's management identifies the specific risks that could impact meeting the criteria and establishes the necessary controls to address these risks.

Information and Communications Systems

Information and communication are integral components of Mango Practice Management's internal control system. This process involves identifying, capturing, and sharing information in the necessary form and timeframe to effectively conduct, manage, and control the organization's operations. It encompasses the primary classes of transactions within the organization, including the reliance on and complexity of information technology. At Mango, information is identified, captured, processed, and reported through various information systems, as well as through ongoing communication with clients, vendors, regulators, and employees.

Meetings are held to discuss operational efficiencies within specific functional areas and to communicate new policies, procedures, controls, and other strategic initiatives across the organization. Additionally, bi-annual town hall meetings are conducted at each geographic location to provide staff with updates on the company and address key issues impacting the organization and its employees. These town halls are led by senior executives who share information gathered from formal automated information systems and informal data sources, as well as insights from conversations with internal and external stakeholders. General updates to company-wide security policies and procedures are typically communicated to relevant Mango personnel via email.

Specific information systems used to support Mango's MT system are described in the Description of Services section above.

Monitoring Controls

Mango Practice Management's management team monitors controls to ensure they operate as intended and adapts them as conditions change. Management conducts ongoing monitoring activities to continuously assess the effectiveness of internal controls over time. Corrective actions are taken as necessary to address any deviations from company policies and procedures. Employee activities and adherence to company policies and procedures are also monitored through ongoing and separate evaluation activities.

On-Going Monitoring

Mango's management conducts regular quality assurance monitoring, with additional training provided as needed based on monitoring results. These activities help initiate corrective actions through department meetings, internal conference calls, and informal notifications.

Close involvement by upper management in Mango's operations helps identify significant variances from expectations regarding internal controls. When control weaknesses are suspected, upper management evaluates the facts and circumstances and determines appropriate actions based on whether the issue is isolated or requires broader procedural or personnel changes. This process aims to ensure legal compliance and maximize the performance of Mango's personnel.

Reporting Deficiencies

An internal tracking tool is used to document and track the results of ongoing monitoring activities. Escalation procedures are in place to notify management of any identified risks, with high-rated risks addressed immediately. Corrective actions, when necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are conducted for management to review reported deficiencies and the status of corrective actions.

Changes to the System in the Last Three Months

No significant changes have occurred to the services provided to user entities in the three months preceding the end of the review period.

Incidents in the Last Three Months

No significant incidents have occurred to the services provided to user entities in the three months preceding the end of the review period.

Criteria Not Applicable to the System

All Common/security criteria was applicable to the Mango Practice Management Software Services.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS and GCP at the multiple facilities.

Subservice Description of Services

AWS and GCP provide cloud hosting services for the in-scope services provided by Mango.

Complementary Subservice Organization Controls

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

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.
		Physical access to data centers is reviewed on a quarterly basis by the appropriate personnel.
		Physical access points to server locations are recorded by a closed-circuit television camera (CCTV). Images are retained for 90 days unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.

The following subservice organization controls should be implemented by 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	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 facilities, 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 cabinet) have been implemented and are administered to restricted access to authorized individuals.
		The datacenter facility is monitored 24x7 by security personnel.

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

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

COMPLEMENTARY USER ENTITY CONTROLS

Mango Practice Management'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 Mango Practice Management's services to be solely achieved by Mango Practice Management control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Mango Practice Management'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 maintaining the confidentiality and security of their usernames, passwords, and other authentication mechanisms (e.g., multi-factor authentication devices).
2. User entities must ensure that only authorized personnel access Mango Practice Management systems and must deactivate accounts when users no longer require access.
3. User entities must immediately notify Mango Practice Management of any actual or suspected information security breaches, including compromised user accounts or systems used for integrations and secure file transfers.
4. User entities are responsible for maintaining their own system(s) of record and ensuring the accuracy and completeness of the data transmitted to or processed by Mango Practice Management.
5. User entities must provide Mango Practice Management with a list of authorized personnel to approve security and system configuration changes related to data transmission or integrations.
6. User entities are responsible for supervising, managing, and controlling the use of Mango Practice Management's services by their personnel to ensure compliance with organizational policies.
7. User entities must develop and maintain their own disaster recovery and business continuity plans to address scenarios where Mango Practice Management services may be temporarily inaccessible.
8. User entities are responsible for notifying Mango Practice Management promptly of any changes to technical or administrative contact information to ensure uninterrupted communication.
9. User entities are responsible for understanding and complying with their contractual obligations to Mango Practice Management, including adherence to agree upon service terms and conditions.
10. User entities must ensure that their use of Mango Practice Management services complies with all applicable legal and regulatory requirements relevant to their industry.

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

Common Criteria (to all 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 Mango Practice Management's description of the system. Any applicable trust services criteria that are not addressed by control activities at Mango Practice Management are described within Section 4 and within the Subservice Organization 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 Mango was limited to the Trust Services Criteria, related criteria and control activities specified by the management of Mango and did not encompass all aspects of Mango'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, procedures, the code of ethics and the employee handbook.	Inspected the employee handbook, code of ethics, information security policies and procedures and the entity's intranet to determine that core values were communicated from executive management to personnel through policies, procedures, the code of ethics and the employee handbook.	No exceptions noted.
		An employee handbook and code of ethics are documented to communicate workforce conduct standards and enforcement procedures.	Inspected the employee handbook and code of ethics to determine that an employee handbook and code of ethics were documented to communicate workforce conduct standards and enforcement procedures.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook and code of ethics.	Inquired of the Director of Human Resources regarding new hire employee handbook and code of ethics acknowledgements to determine that upon hire, personnel were required to acknowledge the employee handbook and code of ethics.	No exceptions noted.
			Inspected the employee handbook and code of ethics to determine that upon hire, personnel were required to acknowledge the employee handbook and code of ethics.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the signed employee manual handbook and code of ethics acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of ethics.	Testing of the control activity disclosed that there were no new hires during the review period.
		Prior to employment, personnel are required to complete a background check.	Inquired of the Director of Human Resources regarding background checks to determine that prior to employment, personnel were required to complete a background check.	No exceptions noted.
			Inspected the background policies and procedures to determine that prior to employment, personnel were required to complete a background check.	No exceptions noted.
			Inspected the completed background check form for a sample of new hires to determine that prior to employment, personnel were required to complete a background check.	Testing of the control activity disclosed that there were no new hires during the review period.
		Personnel are required to acknowledge the employee handbook on an annual basis.	Inspected the signed employee handbook acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook 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**
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
		Sanction policies, which include suspension and termination, are in place for employee misconduct.	Inspected the sanction policies to determine that sanction policies, which include 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 employee handbook to determine that employees, third-parties, and customers were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Executive management roles and responsibilities are documented and reviewed annually.	Inspected the executive management job descriptions including revision dates to determine that executive management roles and responsibilities were documented and reviewed annually.	No exceptions noted.
		Executive management defines and documents the skills and expertise needed among its members.	Inspected the executive management job descriptions to determine that executive management defined and documented the skills and expertise needed among its members.	No exceptions noted.

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 maintains independence from those that operate the key controls implemented within the environment.	Inspected the organizational chart and the completed internal controls matrix to determine that executive management maintained independence from those that operate the key controls implemented within the environment.	No exceptions noted.
		Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	Inspected management meeting agenda to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.
		Executive management evaluates the skills and competencies of those that operate the internal controls implemented within the environment annually.	Inspected the performance 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 implemented within the environment annually.	No exceptions noted.
		Operational management assigns responsibility for and monitors the effectiveness and performance of internal controls implemented within the environment.	Inspected the completed internal controls matrix and management meeting agenda to determine that operational management assigned responsibility for and monitored the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Roles and responsibilities defined in written job descriptions consider and address specific requirements relevant to the system.	Inspected the job description for a sample of job roles to determine that roles and responsibilities defined in written job descriptions considered and addressed specific requirements relevant to the system.	No exceptions noted.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Prior to employment, personnel are required to complete a background check.	Inquired of the Director of Human Resources regarding background checks to determine that prior to employment, personnel were required to complete a background check.	No exceptions noted.
			Inspected the background policies and procedures to determine that prior to employment, personnel were required to complete a background check.	No exceptions noted.
			Inspected the completed background check form for a sample of new hires to determine that prior to employment, personnel were required to complete a background check.	Testing of the control activity disclosed that there were no new hires during the review period.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.	Inspected the employee performance evaluation policies and procedures and competency and training requirements policies and procedures to determine that policies and procedures were in place that outlined the performance evaluation process as well as the competency and training requirements for personnel.	No exceptions noted.
		The entity evaluates the competencies and experience of candidates prior to hiring.	Inquired of the Director of Human Resources regarding candidate evaluations to determine that prior to employment, personnel were required to complete a background check.	No exceptions noted.
			Inspected the recruitment policies and procedures to determine that the entity evaluated the competencies and experience of candidates prior to hiring.	No exceptions noted.
			Inspected the resume for a sample of new hires to determine that the entity evaluated the competencies and experience of candidates prior to hiring.	Testing of the control activity disclosed that there were no new hires during the review period.
		Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer process.	Inquired on the Director of Human Resources regarding candidate evaluations to determine that job requirements were documented in the job descriptions and candidates' abilities to meet these requirements were evaluated as part of the hiring or transfer process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the job description for a sample of job roles and recruitment policies and procedures to determine that job requirements were documented in the job descriptions and candidates' abilities to meet these requirements were evaluated as part of the hiring or transfer process.	No exceptions noted.
			Inspected the job description for a sample of job roles and resume for a sample of new hires to determine that job requirements were documented in the job descriptions and candidates' abilities to meet these requirements were evaluated as part of the hiring or transfer process.	Testing of the control activity disclosed that there were no new hires during the review period.
		The entity has a recruiting department that is responsible for attracting individuals with competencies and experience that align with the entity's goals and objectives.	Inspected the recruiting policies and procedures to determine that the entity had a recruiting department that was responsible for attracting individuals with competencies and experience that aligned with the entity's goals and objectives.	No exceptions noted.
		Employees are required to attend continued training annually that relates to their job role and responsibilities.	Inspected the training completion log 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 uses an outside vendor to assist with its continued training of employees.	Inspected the third-party training content to determine that executive management used an outside vendor to assist with its continued training of employees.	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 employee performance evaluation policies and procedures to determine that as part of the performance evaluation process, the entity rewarded its personnel for exceeding expectations and performed disciplinary actions for its employees who do not meet expectations as it relates to their job role and responsibilities.	No exceptions noted.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Personnel are required to acknowledge the employee handbook on an annual basis.	Inspected the signed employee handbook acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook on an annual basis.	No exceptions noted.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
		Sanction policies, which include suspension and termination, are in place for employee misconduct.	Inspected the sanction policies to determine that sanction policies, which include suspension and termination, were in place for employee misconduct.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		As part of the performance evaluation process, the entity rewards its personnel for exceeding expectations and performs disciplinary actions for its employees who do not meet expectations as it relates to their job role and responsibilities.	Inspected the employee performance evaluation policies and procedures to determine that as part of the performance evaluation process, the entity rewarded its personnel for exceeding expectations and performed disciplinary actions for its employees who do not meet expectations as it relates to their job role and responsibilities.	No exceptions noted.
		Executive management has established performance measures, including the incentives and rewards for exceeding expectations, as it relates to job roles and responsibilities.	Inspected the employee performance evaluation policies and procedures to determine that executive management established performance measures, including the incentives and rewards for exceeding expectations, as it relates to job roles and responsibilities.	No exceptions noted.
		Executive management reviews the job requirements and responsibilities documented within job descriptions annually and makes updates, if necessary.	Inspected the job description including the revision date for a sample of job roles to determine that executive management reviewed the job requirements and responsibilities documented within job descriptions annually and made updates, if necessary.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	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 Team Lead 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.
			Inspected the edit check configurations to determine that edits checks were in place to prevent incomplete or incorrect data from being entered into the system.	No exceptions noted.
		Data flow diagrams are documented and maintained by management to identify the relevant internal and external information sources of the system.	Inspected the data flow diagram to determine that data flow diagrams were documented and maintained by management to identify the relevant internal and external information sources of the system.	No exceptions noted.

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 code repository configurations, IPS configurations, encryption methods and configurations and 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 is only retained for as long as required to perform the required system functionality, service or use.	Inspected the Terms of Service agreement to determine that data was retained for only as long as required to perform the required system functionality, service or use.	No exceptions noted.
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Upon hire, personnel are required to acknowledge the employee handbook and code of ethics.	Inquired of the Director of Human Resources regarding new hire employee handbook and code of ethics acknowledgements to determine that upon hire, personnel were required to acknowledge the employee handbook and code of ethics.	No exceptions noted.
			Inspected the employee handbook and code of ethics to determine that upon hire, personnel were required to acknowledge the employee handbook and code of ethics.	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 signed employee manual handbook and code of ethics acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of ethics.	Testing of the control activity disclosed that there were no new hires during the review period.
		Personnel are required to acknowledge the employee handbook on an annual basis.	Inspected the signed employee handbook acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook on an annual basis.	No exceptions noted.
		Employees, third-parties, and customers are directed on how to report unethical behavior in a confidential manner.	Inspected the employee handbook to determine that employees, third-parties, and customers were directed on how to report unethical behavior in a confidential manner.	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 ethics and employee handbook are made available to personnel through the entity's intranet.	Observed the entity's intranet to determine that the entity's policies and procedures, code of ethics 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**
			Inspected the entity's intranet to determine that the entity's policies and procedures, code of ethics and employee handbook were made available to personnel through the entity's intranet.	No exceptions noted.
		Upon hire, personnel are required to complete information security awareness training.	Inquired of the IT Manager regarding information security awareness training to determine that upon hire, personnel were required to complete information security awareness training.	No exceptions noted.
			Inspected the training policies and procedures to determine that upon hire, personnel were required to complete information security awareness training.	No exceptions noted.
			Inspected the information security awareness training completion form for a sample of new hires to determine that upon hire, personnel were required to complete information security awareness training.	Testing of the control activity disclosed that there were no new hires during the review period.
		Current employees are required to complete information security awareness training annually.	Inspected the information security awareness training completion log for a sample of current employees to determine that current employees were required to complete information security awareness training annually.	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**
		Executive management meets annually with operational management to discuss the entity's objectives as well as roles and responsibilities.	Inspected a PowerPoint 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.
		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.
		The information security policies and procedures that communicate the system commitments and requirements of external users are provided to external users prior to allowing them access to the system.	Inspected the information security policies and procedures to determine that the information security policies and procedures that communicated the system commitments and requirements of external users were provided to external users prior to allowing them access to the system.	No exceptions noted.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	Employees, third-parties, and customers are directed on how to report unethical behavior in a confidential manner.	Inspected the employee handbook to determine that employees, third-parties, and customers were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The entity establishes organizational strategies and objectives that are used to determine entity structure and performance metrics.	Inspected the organizational chart, employee performance evaluation policies and procedures and the entity's documented objectives and strategies to determine that the entity established organizational strategies and objectives that were used to determine entity structure and performance metrics.	No exceptions noted.
		Executive management has documented objectives that are specific, measurable, attainable, relevant and time-bound (SMART).	Inspected the entity's documented objectives and strategies to determine that executive management had documented objectives that were specific, measurable, attainable, relevant and time-bound (SMART).	No exceptions noted.
		Executive management identifies and assesses risks that could prevent the entity's objectives from being achieved.	Inspected the risk assessment and management policies and procedures and completed risk assessment to determine that executive management identified and assessed risks that could prevent the entity's objectives from being achieved.	No exceptions noted.
		Executive management reviews policies, procedures and other control documents for alignment to the entity's objectives on an annual basis.	Inspected management meeting agenda 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**
		Executive management has established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	Inspected the documented key performance indicators for operational and internal controls effectiveness to determine that executive management established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	No exceptions noted.
		Responsible parties are defined and assigned to coordinate and monitor compliance and audit activities.	Inspected the Director of Information Security job description to determine that responsible parties were defined and assigned to coordinate and monitor compliance and audit activities.	No exceptions noted.
		The entity has defined the desired level of performance and operation in order to achieve the established entity objectives.	Inspected the documented key performance indicators for operational and internal controls effectiveness to determine that the entity defined the desired level of performance and operation in order to achieve the established entity objectives.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Key performance indicators of both the business performance and employee performance are developed in alignment with entity objectives and strategies.	Inspected the employee performance evaluation policies and procedures, the entity's documented objectives and strategies and the documented key performance indicators for operational and internal controls effectiveness to determine that key performance indicators of both the business performance and employee performance were developed in alignment with entity objectives and strategies.	No exceptions noted.
		Business plans and budgets align with the entity's strategies and objectives.	Inspected the entity's business plans, budget, and documented objectives and strategies to determine that business plans and budgets aligned with the entity's strategies and objectives.	No exceptions noted.
		Entity strategies, objectives and budgets are assessed on an annual basis.	Inspected a PowerPoint deck to determine that entity strategies, objectives and budgets were assessed on an annual basis.	No exceptions noted.
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Documented policies and procedures are in place to guide personnel when performing a risk assessment.	Inspected the risk assessment and management policies and procedures to determine that documented policies and procedures were in place to guide personnel when performing a risk assessment.	No exceptions noted.

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 and management policies and procedures to determine that management defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	No exceptions noted.
		A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.

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

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

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

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

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

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		On an annual basis, management reviews the controls implemented within the environment for compliance and operational effectiveness and identifies potential control gaps and weaknesses.	Inspected the completed internal controls matrix to determine that on an annual basis, management reviewed the controls implemented within the environment for compliance and operational effectiveness and identified potential control gaps and weaknesses.	No exceptions noted.
		Logical access reviews are performed annually.	Inquired of the VP of Development regarding user access reviews to determine that logical access reviews were performed annually.	No exceptions noted.
			Inspected the completed access review for the in-scope systems to determine that physical and logical access reviews were performed annually.	No exceptions noted.
		A data backup restoration test is performed annually.	Inquired of the VP of Development regarding restoration testing to determine that a data backup restoration test was performed annually.	No exceptions noted.
			Inspected the completed backup restoration test to determine that a data backup restoration test was performed annually.	No exceptions noted.
		Internal and external vulnerability scans are performed quarterly and remedial actions are taken where necessary.	Inquired of the VP of Development regarding 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**
			Inspected the vulnerability scanning policies and procedures and completed vulnerability scan results 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 critical vulnerabilities identified by the vulnerability scans to determine that internal and external vulnerability scans were performed quarterly and remedial actions were taken where necessary.	Testing of the control activity disclosed no vulnerabilities occurred during the review period.
		A third-party performs a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	Inspected the completed penetration test results to determine that a third-party performed a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	No exceptions noted.
		Management obtains and reviews attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Inquired of the VP of Development regarding vendor reviews to determine that management obtained and reviewed attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	No exceptions noted.

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 completed third-party attestation reports or vendor questionnaire for a sample of third-parties that the entity has a relationship with to determine that management obtained and reviewed attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Testing of the control activity disclosed that management did not obtain and review attestation reports and vendor questionnaires to evaluate the effectiveness of controls within the vendor or third-party's environment for three of five third-parties sampled.
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 management meeting agenda to determine that senior management assessed the results of the compliance, control and risk assessments performed on the environment.	No exceptions noted.
		Senior management is made aware of high-risk vulnerabilities, deviations and controls gaps identified as part of the compliance, control and risk assessments performed.	Inspected management meeting agenda 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.	Inquired of the VP of Development regarding vulnerabilities, deviations and control failures/gaps 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 vulnerability management policy 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 various assessments 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.
			Inspected the supporting incident tickets for a sample of vulnerabilities identified from a penetration test to determine that vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment were communicated to those parties responsible for taking corrective actions.	Testing of the control activity disclosed that there were no vulnerabilities identified from the various assessments performed on the environment during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment are documented, investigated, and addressed.	Inquired of the VP of Development regarding vulnerabilities, deviations and control failures/gaps 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 vulnerability management policy 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 various assessments 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.

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 tickets for a sample of vulnerabilities identified from a penetration test to determine that vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment were documented, investigated and addressed.	Testing of the control activity disclosed that there were no vulnerabilities identified from the various assessments performed on the environment during the review period.
		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.	Inquired of the VP of Development regarding vulnerabilities, deviations and control failures/gaps 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 vulnerability management policy 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 various assessments 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 tickets for a sample of vulnerabilities identified from a penetration test to determine that vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment were addressed by those parties responsible for taking corrective actions.	Testing of the control activity disclosed that there were no vulnerabilities identified from the various assessments performed on the environment during the review period.
		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 agenda 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.	Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	Inspected the risk assessment and management policies and procedures and completed risk assessment to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
		As part of the risk assessment process, controls within the environment are modified and implemented to mitigate identified vulnerabilities, deviations and control gaps.	Inspected the completed risk assessment to determine that as part of the risk assessment process, controls within the environment were modified and implemented to mitigate identified vulnerabilities, deviations and control gaps.	No exceptions noted.
		Controls within the environment are modified and implemented to mitigate vulnerabilities, deviations and control failures/gaps identified as part of the various evaluations performed.	Inquired of the VP of Development regarding vulnerabilities, deviations and 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.
			Inspected the vulnerability management policy 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 various assessments 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 tickets for a sample of vulnerabilities identified from a penetration test to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control failures/gaps identified as part of the various evaluations performed.	Testing of the control activity disclosed that there were no vulnerabilities identified from the various assessments performed on the environment during the review period.
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Inspected the organizational chart and the completed internal controls matrix to determine that performance of the internal controls implemented within the environment were assigned to appropriate process owners and operational personnel based on roles and responsibilities.	No exceptions noted.
		Management has documented the relevant controls in place for each key business or operational process.	Inspected the completed internal controls matrix to determine that management documented the relevant controls in place for each key business or operational process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	Inspected the completed internal controls matrix to determine that management incorporated a variety of controls into their environment that included manual, automated, preventive, detective, and corrective controls.	No exceptions noted.
		Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the business continuity and disaster recovery plans to determine that business continuity and disaster recovery plans were developed and updated on an annual basis.	No exceptions noted.
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed business continuity and disaster recovery test results to determine that the business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.
		An analysis of incompatible operational duties is performed on at least an annual basis, and where incompatible responsibilities are identified, compensating controls are put into place.	Inspected the organizational chart, the completed internal controls matrix, and management notes to determine that an analysis of incompatible operational duties was performed on at least an annual basis, and where incompatible responsibilities were identified, compensating controls were put into place.	No exceptions noted.

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.	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 relationship and linkage between business processes, the relevant technologies used to support the business processes, and the controls in place to help secure those business processes.	Inspected the completed internal controls matrix to determine that management documented the relationship and linkage between business processes, the relevant technologies used to support the business processes, and the controls in place to help secure those business processes.	No exceptions noted.
		Management has documented the controls implemented around the entity's technology infrastructure.	Inspected the completed internal controls matrix to determine that management documented the controls implemented around the entity's technology infrastructure.	No exceptions noted.
		Management has established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.	Inspected the completed internal controls matrix to determine that management established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.	No exceptions noted.

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 established controls around the acquisition, development and maintenance of the entity's technology infrastructure.	No exceptions noted.
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet.	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**
		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.
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Inspected the organizational chart and the completed internal controls matrix to determine that performance of the internal controls implemented within the environment were assigned to appropriate process owners and operational personnel based on roles and responsibilities.	No exceptions noted.
		The organizational and information security policies and procedures detail the day-to-day activities to be performed by personnel.	Inspected the organizational and information security policies and procedures to determine that the organizational and information security policies and procedures detailed the day-to-day activities to be performed by personnel.	No exceptions noted.
		Management has implemented controls that are built into the organizational and information security policies and procedures.	Inspected the organizational and information security policies and procedures and the completed internal controls matrix to determine that management implemented controls that were built into the organizational and information security policies and procedures.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Process owners and key management are assigned ownership to each key internal control implemented within the entity's environment.	Inspected the completed internal controls matrix to determine that process owners and key management were assigned ownership to each key internal control implemented within the entity's environment.	No exceptions noted.
		Process owners and management operate the controls implemented within the entity's environment based on the frequency defined in the organizational and information security policies and procedures.	Inspected the organizational and information security policies and procedures and the completed internal controls matrix to determine that process owners and management operated the controls implemented within the entity's environment based on the frequency defined in the organizational and information security policies and procedures.	No exceptions noted.
		The effectiveness of the internal controls implemented within the environment is evaluated annually.	Inspected the meeting agenda to determine that the effectiveness of the internal controls implemented within the environment was evaluated annually.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the network user listing and access rights to determine that network user access was restricted via role based security privileges defined within the access control system.	No exceptions noted.
		Network administrative access is restricted to authorized personnel.	Inquired of the VP of Development regarding administrative access to determine that network administrative access was restricted to authorized personnel.	No exceptions noted.
			Inspected the network administrator listing and access rights to determine that network administrative access was restricted to authorized personnel.	No exceptions noted.
		Network users are authenticated via individually-assigned user accounts and passwords.	Inspected the authentication settings to determine that network users were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.
		The network is configured to enforce password requirements that include: • Password history • Password length • Complexity	Inspected the network password settings to determine that the network was configured to enforce password requirements that included: • Password history • 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**
		Network account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold	Inspected the network account lockout settings to determine that network account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold	No exceptions noted.
		Network audit logging configurations are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the network audit logging configurations and an example network audit log extract to determine that network audit logging configurations were in place that included: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.
		Network audit logs are maintained for review when needed.	Inquired of the VP of Development regarding network audit logs to determine that network audit logs were maintained for review when needed.	No exceptions noted.
			Inspected an example network audit log extract to determine that network audit logs were maintained 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 server user access is restricted via role based security privileges defined within the access control system.	Inquired of the VP of Development regarding production server access to determine that production server user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
			Inspected the production server user listing and access roles for a sample of production servers to determine that production server user access was restricted via role based security privileges defined within the access control system.	No exceptions noted.
		Production server administrative access is restricted to authorized personnel.	Inquired of the VP of Development regarding administrative access to determine that production server administrative access was restricted to authorized personnel.	No exceptions noted.
			Inspected the production server administrator listing and access roles for a sample of production servers to determine that production servers administrative access was restricted to authorized personnel.	No exceptions noted.
		Production server users are authenticated via individually-assigned user accounts and passwords.	Inspected the production server user listings and password configurations for production servers to determine that production servers users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Production servers are configured to enforce password requirements that include: • Password history • Maximum password age • Password length • Complexity	Inspected the password configurations for production servers to determine that the production servers were configured to enforce password requirements that included: • Password history • Maximum password age • Password length • Complexity	No exceptions noted.
		Production server audit logging configurations are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the audit logging configurations for production servers and an example production server audit log extract to determine that production server audit logging configurations were in place that included: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.
		Production server audit logs are maintained for review when needed.	Inquired of the VP of Development regarding production server audit logs to determine that production server audit logs were maintained 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 production server audit log extract to determine that production server audit logs were maintained for review when needed.	No exceptions noted.
		Production database user access is restricted via role based security privileges defined within the access control system.	Inquired of the VP of Development regarding production database access to determine that production databases 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 for a sample of production databases to determine that production databases user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Production database administrative access is restricted to authorized personnel.	Inquired of the VP of Development regarding administrative access to determine that database administrative access was restricted to authorized personnel.	No exceptions noted.
			Inspected the production database administrator listing and access roles for production databases to determine that production databases 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**
		Production database users are authenticated via individually-assigned user accounts and passwords.	Inspected the production database user listings and password configurations for production databases to determine that production databases users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
		Production databases are configured to enforce password requirements that include: • Password length • Complexity	Inspected the password configurations for production databases to determine that production databases were configured to enforce password requirements that included: • Password length • Complexity	No exceptions noted.
		Production database audit logging configurations are in place to log user activity and system events.	Inspected the production databases audit logging configurations and an example production database audit log extract to determine that production databases audit logging configurations were in place to log user activity and system events.	No exceptions noted.
		Production database audit logs are maintained for review when needed.	Inquired of the VP of Development regarding the production databases audit logs to determine that the production databases audit logs were maintained 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 production database audit log extract to determine that production databases audit logs were maintained for review when needed.	No exceptions noted.
		Production application user access is restricted via role-based security privileges defined within the access control system.	Inquired of the VP of Development regarding production application access to determine that production application user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
			Inspected the production application user listing and access roles to determine that production application user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Production application administrative access is restricted to authorized personnel.	Inquired of the VP of Development regarding administrative access to determine that production application administrative access was restricted to authorized personnel.	No exceptions noted.
			Inspected the production application administrator listing and access roles to determine that production 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**
		Production application users are authenticated via individually-assigned user accounts and passwords.	Inspected the production application user listing and password configurations to determine that production application users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
		The production application is configured to enforce password requirements that include: • Password length • Complexity • MFA	Inspected the production application password configurations to determine that applications were configured to enforce password requirements that included: • Password length • Complexity • MFA	No exceptions noted.
		Production application audit logging configurations are in place to log user activity and system events.	Inspected the production application audit logging configurations and an example production application audit log extract to determine that production application audit logging configurations were in place to log user activity and system events.	No exceptions noted.
		Production application audit logs are maintained for review when needed.	Inquired of the VP of Development regarding application audit logs to determine that application audit logs were maintained 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 production application audit log extract to determine that production application audit logs were maintained for review when needed.	No exceptions noted.
		VPN user access is restricted via role based security privileges defined within the access control system.	Inquired of the VP of Development 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 and access rights to determine that VPN user access was restricted via role based security privileges defined within the access control system.	No exceptions noted.
		The ability to administer VPN access is restricted to authorized personnel.	Inquired of the VP of Development regarding administrative access to the VPN to determine that the ability to administer VPN access was restricted to authorized personnel.	No exceptions noted.
			Inspected the VPN administrator listing to determine that the ability to administer VPN access was restricted to authorized personnel.	No exceptions noted.
		Users are authenticated via multi-factor authentication prior to being granted remote access to the environment.	Inspected the VPN authentication settings to determine that VPN users were authenticated via multi-factor authentication prior to being granted remote access to the 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**
		The entity's various networks are segmented to keep information and data isolated and restricted to authorized personnel.	Inspected 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.
		Data coming into the environment is secured and monitored through the use of firewalls and an IPS.	Inspected the IPS configurations and centralized firewall rule sets to determine that data coming into the environment was secured and monitored through the use of firewalls IPS.	No exceptions noted.
		Server certificate-based authentication is used as part of the Transport Layer Security (TLS) encryption with a trusted certificate authority.	Inspected the encryption configurations for data in transit and to determine that server certificate-based authentication was used as part of the 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.	Inspected the encryption policies and procedures to determine that encryption keys were required to be protected during generation, storage, use, and destruction.	No exceptions noted.
		Logical access reviews are performed annually.	Inquired of the VP of Development regarding user access reviews to determine that logical access reviews were performed 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**
			Inspected the completed access review for the in-scope systems to determine that logical access reviews were performed annually.	No exceptions noted.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inquired of the IT 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 access management policies and procedures 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 form 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.	Testing of the control activity disclosed that there were no new hires during the review period.
		Logical access to systems is revoked as a component of the termination process.	Inquired of the IT 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 access management policies and procedures 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 form for a sample of terminated employees to determine that logical access to systems was revoked from personnel as a component of the termination process.	Testing of the control activity disclosed that there were no employees terminated during the review period.
		Privileged access to add, remove, or modify access to user accounts is restricted to authorized personnel.	Inquired of the VP of Development regarding privileged access to sensitive resources to determine that privileged access to sensitive resources add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.
			Inspected the listing of privileged users to the in-scope systems to determine that privileged access to add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the access management policies and procedures 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 form 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.	Testing of the control activity disclosed that there were no new hires during the review period.
		Logical access to systems is revoked as a component of the termination process.	Inquired of the IT 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 access management policies and procedures 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 form for a sample of terminated employees to determine that logical access to systems was revoked from personnel as a component of the termination process.	Testing of the control activity disclosed that there were no employees terminated during the review period.
		Privileged access to add, remove, or modify access to user accounts is restricted to authorized personnel.	Inquired of the VP of Development regarding privileged access to sensitive resources to determine that privileged access to sensitive resources add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.
			Inspected the listing of privileged users to the in-scope systems to determine that privileged access to add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	An analysis of incompatible operational duties is performed on at least an annual basis, and where incompatible responsibilities are identified, compensating controls are put into place.	Inspected the organizational chart, the completed internal controls matrix, and management notes to determine that an analysis of incompatible operational duties was performed on at least an annual basis, and where incompatible responsibilities were identified, compensating controls were put into place.	No exceptions noted.

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 policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
		Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the VP of Development regarding privileged access to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
			Inspected the listings of privileged users to the network, operating system, database and application to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
		Logical access reviews are performed annually.	Inquired of the VP of Development regarding user access reviews to determine that logical access reviews were performed annually.	No exceptions noted.
			Inspected the completed access review for the in-scope systems to determine that logical access reviews were performed annually.	No exceptions noted.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inquired of the IT 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the access management policies and procedures 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 form 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.	Testing of the control activity disclosed that there were no new hires during the review period.
		Logical access to systems is revoked as a component of the termination process.	Inquired of the IT 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 access management policies and procedures 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 form for a sample of terminated employees to determine that logical access to systems was revoked from personnel as a component of the termination process.	Testing of the control activity disclosed that there were no employees terminated during the review period.
		Privileged access to add, remove, or modify access to user accounts is restricted to authorized personnel.	Inquired of the VP of Development regarding privileged access to sensitive resources to determine that privileged access to sensitive resources add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.
			Inspected the listing of privileged users to the in-scope systems to determine that privileged access to add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	This criterion is the responsibility of the subservice organization. Refer to the "Subservice Organizations" section above for controls managed by the subservice organization.	Not applicable.	Not applicable.

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 terms of service agreement to determine that policies and procedures were in place to guide personnel in data, hardware and software disposal and destruction.	No exceptions noted.
		The entity purges data stored on cloud backups, per a defined schedule.	Inspected the backup schedule and configurations to determine that the entity purged data stored on cloud backups per a defined schedule.	No exceptions noted.
		Data that is no longer required is disposed of and rendered unreadable to meet the entity's objectives.	Inquired of the VP of Development regarding data disposal 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 Terms of Service agreement 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 Terms of Service agreement and destruction certificate for a sample of requests to dispose of data, purge a system, or physically destroy a system to determine that data that was no longer required was disposed of and rendered unreadable to meet the entity's objectives.	Testing of the control activity disclosed that there were no requests dispose of data, purge a system, or physically destroy a system during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	VPN user access is restricted via role based security privileges defined within the access control system.	Inquired of the VP of Development 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 and access rights to determine that VPN user access was restricted via role based security privileges defined within the access control system.	No exceptions noted.
		Users are authenticated via multi-factor authentication prior to being granted remote access to the environment.	Inspected the VPN authentication settings to determine that VPN users were authenticated via multi-factor authentication prior to being granted remote access to the system.	No exceptions noted.
		Server certificate-based authentication is used as part of the Transport Layer Security (TLS) encryption with a trusted certificate authority.	Inspected the encryption configurations for data in transit and to determine that server certificate-based authentication was used as part of the 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.
		Network address translation (NAT) functionality is utilized to manage internal IP addresses.	Inspected the NAT configurations to determine that NAT functionality was utilized to manage internal IP addresses.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		VPN, 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, TLS and other encryption technologies were used for defined points of connectivity.	No exceptions noted.
		Transmission of digital output beyond the boundary of the system is encrypted.	Inspected the encryption configurations for data in transit and digital certificates to determine that transmission of digital output beyond the boundary of the system was encrypted.	No exceptions noted.
		Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	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 VP of Development 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 rights to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the network diagram and centralized firewall rule sets for the production servers to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram and centralized firewall rule sets for the production servers to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		An IPS is utilized to analyze network events and report possible or actual network security breaches.	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 prevention.	Inspected the IPS configurations and third-party contract to determine that the IPS was configured to notify personnel upon intrusion prevention.	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 dashboard console and centralized antivirus configurations to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the centralized antivirus software configurations 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 weekly basis.	Inspected the centralized antivirus software configurations to determine that the antivirus software was configured to scan workstations on a weekly basis.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the removable media policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Server certificate-based authentication is used as part of the Transport Layer Security (TLS) encryption with a trusted certificate authority.	Inspected the encryption configurations for data in transit and to determine that server certificate-based authentication was used as part of the 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Network address translation (NAT) functionality is utilized to manage internal IP addresses.	Inspected the NAT configurations to determine that NAT functionality was utilized to manage internal IP addresses.	No exceptions noted.
		VPN, 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, TLS and other encryption technologies were used for defined points of connectivity.	No exceptions noted.
		Transmission of digital output beyond the boundary of the system is encrypted.	Inspected the encryption configurations for data in transit and digital certificates to determine that transmission of digital output beyond the boundary of the system was encrypted.	No exceptions noted.
		Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	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 VP of Development regarding access to stored data to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the database user listing and access rights to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the network diagram and centralized firewall rule sets for the production servers to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram and centralized firewall rule sets for the production servers to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		An IPS is utilized to analyze network events and report possible or actual network security breaches.	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 prevention.	Inspected the IPS configurations and third-party contract to determine that the IPS was configured to notify personnel upon intrusion prevention.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the removable media policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
		System data is encrypted during the replication process between cloud environments.	Inspected the backup replication configurations to determine that system data was replicated and encrypted via the cloud daily.	No exceptions noted.
		The ability to restore backups is restricted to authorized personnel.	Inquired of the VP of Development regarding restoring backed up data to determine that the ability to restore backups was restricted to authorized personnel.	No exceptions noted.
			Inspected the listing of users with the ability to restore backups to determine that the ability to restore backups was restricted to authorized personnel.	No exceptions noted.
		Backup media is stored in an encrypted format.	Inspected the encryption configurations for an example backup media to determine that backup media was stored in an encrypted format.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Antivirus software is installed on workstations and 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 dashboard console and centralized antivirus configurations to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the centralized antivirus software configurations 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 weekly basis.	Inspected the centralized antivirus software configurations to determine that the antivirus software was configured to scan workstations on a weekly basis.	No exceptions noted.
		The ability to install applications and software on workstations is restricted to authorized personnel.	Inquired of the IT 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.
			Inspected the denial 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 VP of Development regarding the ability to migrate 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the list of 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.
		Code repository is utilized to help detect unauthorized changes within the production environment.	Inspected the code repository configurations to determine that code repository was utilized to help detect unauthorized changes within the production environment.	No exceptions noted.
		The code repository is configured to notify IT personnel via email alert when a change to the production application code files is detected.	Inspected the code repository notification configurations and an example alert generated from the code repository to determine that the code repository was configured to notify IT personnel via email alert when a change to the production application code files was detected.	No exceptions noted.
		Documented change control policies and procedures are in place to guide personnel in the change management process.	Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in the change management process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, code repository configurations, IPS configurations, and centralized firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		Internal and external vulnerability scans are performed quarterly and remedial actions are taken where necessary.	Inquired of the VP of Development regarding vulnerability scans to determine that internal and external vulnerability scans were performed quarterly and remedial actions were taken where necessary.	No exceptions noted.
			Inspected the vulnerability scanning policies and procedures and completed vulnerability scan results 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 critical vulnerabilities identified by the vulnerability scans to determine that internal and external vulnerability scans were performed quarterly and remedial actions were taken where necessary.	Testing of the control activity disclosed no vulnerabilities occurred during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A third-party performs a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	Inspected the completed penetration test results to determine that a third-party performed a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the network diagram and centralized firewall rule sets for the production servers to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram and centralized firewall rule sets for the production servers to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		An IPS is utilized to analyze network events and report possible or actual network security breaches.	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 prevention.	Inspected the IPS configurations and third-party contract to determine that the IPS was configured to notify personnel upon intrusion prevention.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the removable media policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
		Code repository is utilized to help detect unauthorized changes within the production environment.	Inspected the code repository configurations to determine that code repository was utilized to help detect unauthorized changes within the production environment.	No exceptions noted.
		The code repository is configured to notify IT personnel via email alert when a change to the production application code files is detected.	Inspected the code repository notification configurations and an example alert generated from the code repository to determine that the code repository was configured to notify IT personnel via email alert when a change to the production application code files was detected.	No exceptions noted.
		Management defined configuration standards in the information security policies and procedures.	Inspected the information security policies and procedures to determine that management defined configuration standards in the information security policies and procedures.	No exceptions noted.
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations and MSSP contract to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Network audit logging configurations are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the network audit logging configurations and an example network audit log extract to determine that network audit logging configurations were in place that included: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.
		Network audit logs are maintained for review when needed.	Inquired of the VP of Development regarding network audit logs to determine that network audit logs were maintained for review when needed.	No exceptions noted.
			Inspected an example network audit log extract to determine that network audit logs were maintained 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 server audit logging configurations are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the audit logging configurations for production servers and an example production server audit log extract to determine that production server audit logging configurations were in place that included: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.
		Production server audit logs are maintained for review when needed.	Inquired of the VP of Development regarding production server audit logs to determine that production server audit logs were maintained for review when needed.	No exceptions noted.
			Inspected an example production server audit log extract to determine that production server audit logs were maintained for review when needed.	No exceptions noted.
		Production database audit logging configurations are in place to log user activity and system events.	Inspected the production databases audit logging configurations and an example production database audit log extract to determine that production databases audit logging configurations were in place to log user activity and system events.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Production database audit logs are maintained for review when needed.	Inquired of the VP of Development regarding the production databases audit logs to determine that the production databases audit logs were maintained for review when needed.	No exceptions noted.
			Inspected an example production database audit log extract to determine that production databases audit logs were maintained for review when needed.	No exceptions noted.
		Production application audit logging configurations are in place to log user activity and system events.	Inspected the production application audit logging configurations and an example production application audit log extract to determine that production application audit logging configurations were in place to log user activity and system events.	No exceptions noted.
		Production application audit logs are maintained for review when needed.	Inquired of the VP of Development regarding application audit logs to determine that application audit logs were maintained for review when needed.	No exceptions noted.
			Inspected an example production application audit log extract to determine that production application audit logs were maintained 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**
		An IPS is utilized to analyze network events and report possible or actual network security breaches.	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 prevention.	Inspected the IPS configurations and third-party contract to determine that the IPS was configured to notify personnel upon intrusion prevention.	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 dashboard console and centralized antivirus configurations to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the centralized antivirus software configurations 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 weekly basis.	Inspected the centralized antivirus software configurations to determine that the antivirus software was configured to scan workstations on a weekly basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the removable media policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
		Code repository is utilized to help detect unauthorized changes within the production environment.	Inspected the code repository configurations to determine that code repository was utilized to help detect unauthorized changes within the production environment.	No exceptions noted.
		The code repository is configured to notify IT personnel via email alert when a change to the production application code files is detected.	Inspected the code repository notification configurations and an example alert generated from the code repository to determine that the code repository was configured to notify IT personnel via email alert when a change to the production application code files was detected.	No exceptions noted.
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations and MSSP contract to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.
		Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected the information security and incident management policies and procedures to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident management and escalation policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		Management reviews reports on an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes.	Inspected meeting agenda 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.
		Part of this criterion is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident management and escalation policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		The incident response and escalation procedures are reviewed at least annually for effectiveness.	Inspected the revision history of the incident response policies and procedures to determine that the incident response and escalation procedures were reviewed at least annually for effectiveness.	No exceptions noted.
		The incident response policies and procedures define the classification of incidents based on its severity.	Inspected the incident response policies and procedures to determine that the incident response policies and procedures defined the classification of incidents based on its severity.	No exceptions noted.
		Resolution of incidents are documented within the ticket and communicated to affected users.	Inquired of the VP of Development regarding resolution of incidents 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.
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inquired of the VP of Development regarding incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			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.
		A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.	Inquired of the VP of Development regarding security incident analysis to determine that an impact analysis was performed 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 an impact analysis was performed to determine the root cause, system impact, and resolution.	No exceptions noted.
			Inspected the supporting incident ticket for an example critical security incident to determine that an impact analysis was performed to determine the root cause, system impact, and resolution.	Testing of the control activity disclosed that there were no critical incidents during the review period.
		Identified incidents are reviewed, monitored and investigated by an incident response team.	Inquired of the VP of Development regarding incidents to determine that identified incidents were reviewed, monitored and investigated by an incident response team.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that identified incidents were reviewed, monitored and investigated by an incident response team.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that identified incidents were reviewed, monitored and investigated by an incident response team.	Testing of the control activity disclosed that there were no incidents during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Incidents resulting in the unauthorized use or disclosure of personal information are communicated to the affected users.	Inquired of the VP of Development regarding incidents to determine that incidents resulting in the unauthorized use or disclosure of personal information were identified and 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 identified and communicated to the affected users.	No exceptions noted.
			Inspected the in app notification for an example critical security incident that resulted in unauthorized disclosure of personal information to determine that incidents resulting in the unauthorized use or disclosure of personal information were identified and communicated to the affected users.	Testing of the control activity disclosed that there were no incidents during the review period.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident management and escalation policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management reviews reports on an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes.	Inspected meeting agenda to determine that management reviewed reports on an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identified the need for system changes and implementation of additional controls based on incident patterns and root causes.	No exceptions noted.
		The incident response and escalation procedures are reviewed at least annually for effectiveness.	Inspected the revision history of the incident response policies and procedures to determine that the incident response and escalation procedures were reviewed at least annually for effectiveness.	No exceptions noted.
		Resolution of incidents are documented within the ticket and communicated to affected users.	Inquired of the VP of Development regarding resolution of incidents 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inquired of the VP of Development regarding incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			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.
		A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.	Inquired of the VP of Development regarding security incident analysis to determine that an impact analysis was performed to determine the root cause, system impact, and resolution.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that an impact analysis was performed 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 supporting incident ticket for an example critical security incident to determine that an impact analysis was performed to determine the root cause, system impact, and resolution.	Testing of the control activity disclosed that there were no critical incidents during the review period.
		Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are defined and documented.	Inspected the incident response policies and procedures to determine that roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program were defined and documented.	No exceptions noted.
		The actions taken to address identified security incidents are documented and communicated to affected parties.	Inquired of the VP of Development regarding security incidents 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 and release notes 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Documented incident response and escalation procedures are in place to guide personnel in addressing the threats posed by security incidents.	Inspected the incident response policies and procedures to determine that documented incident response and escalation procedures were in place to guide personnel in addressing the threats posed by security incidents.	No exceptions noted.
		Critical security incidents that result in a service/business operation disruption are communicated to those affected through in app notifications.	Inquired of the VP of Development regarding critical security incidents to determine that critical security incidents that result in a service/business operation disruption were communicated to those affected through in app notification.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that critical security incidents that result in a service/business operation disruption were communicated to those affected through in app notification.	No exceptions noted.
			Inspected the in app notification for an example critical security incident that resulted in a service/business operation disruption to determine that critical security incidents that result in a service/business operation disruption were communicated to those affected through in app notification.	Testing of the control activity disclosed that there were no critical 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**
		Remediation actions taken for security incidents are documented within the ticket and communicated to affected users.	Inquired of the VP of Development regarding remediation actions 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 and release notes 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.
		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 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	A data backup restoration test is performed annually.	Inquired of the VP of Development regarding restoration testing to determine that a data backup restoration test was performed annually.	No exceptions noted.
			Inspected the completed backup restoration test to determine that a data backup restoration test was performed annually.	No exceptions noted.
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed business continuity and disaster recovery test results to determine that the business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.
		Management reviews reports on an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes.	Inspected meeting agenda 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 VP of Development regarding security incident analysis to determine that an impact analysis was performed 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 an impact analysis was performed to determine the root cause, system impact, and resolution.	No exceptions noted.
			Inspected the supporting incident ticket for an example critical security incident to determine that an impact analysis was performed to determine the root cause, system impact, and resolution.	Testing of the control activity disclosed that there were no critical incidents during the review period.
		The entity restores system operations for incidents impacting the environment through activities that include, but are not limited to: • Rebuilding systems • Updating software • Installing patches • Removing unauthorized access • Changing configurations	Inspected the information security, incident, and change management policies and procedures, and the system build guides for critical systems to determine that the entity restored system operations for incidents impacting the environment through activities that included, but were not limited to: • Rebuilding systems • Updating software • Installing patches • Removing unauthorized access • Changing configurations	No exceptions noted.
		Data backup and restore procedures are in place to guide personnel in performing backup activities.	Inspected the backup policies and procedures to determine that data backup and restore procedures were in place to guide personnel in performing backup activities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A business continuity and disaster recovery plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	Inspected the business continuity and disaster recovery plans to determine that a business continuity and disaster recovery plan was documented to identify and reduce risks, limited the consequences of damaging incidents, and ensured the timely resumption of essential operations.	No exceptions noted.
		The business continuity and disaster recovery plan and procedures are updated based on disaster recovery plan test results.	Inspected the business continuity and disaster recovery plans and completed business continuity and disaster recovery test results to determine that the business continuity and disaster recovery plan and procedures were updated based on disaster recovery plan test results.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The ability to migrate changes into the production environment is restricted to authorized and appropriate users.	Inquired of the VP of Development regarding the ability to migrate 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.
			Inspected the list of users with the ability to implement changes into the production environment to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users.	No exceptions noted.
		Code repository is utilized to help detect unauthorized changes within the production environment.	Inspected the code repository configurations to determine that code repository was utilized to help detect unauthorized changes within the production environment.	No exceptions noted.
		The code repository is configured to notify IT personnel via email alert when a change to the production application code files is detected.	Inspected the code repository notification configurations and an example alert generated from the code repository to determine that the code repository was configured to notify IT personnel via email alert when a change to the production application code files was detected.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Documented change control policies and procedures are in place to guide personnel in 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 Management Committee and Emergency Change management Committee • Development - Change Requester and Change Manager • Testing - Information Technology Team and Information Security Team • Implementation - Change Implementer	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 Management Committee and Emergency Change management Committee • Development - Change Requester and Change Manager • Testing - Information Technology Team and Information Security Team • Implementation - Change Implementer	No exceptions noted.
		System changes are communicated to both affected internal and external users.	Inspected the newsletter and in-app notification to determine that system changes were communicated to both affected internal and external users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		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 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.
		System patches/security updates follow the standard change management process.	Inspected the patch management policies and procedures to determine that system patches/security updates follow the standard patch management process.	No exceptions noted.
		System patches/security updates are performed on a configured schedule.	Inspected the MSSP Contract Portfolio to determine that system patches/security updates were performed on a configured schedule.	No exceptions noted.
		Development and test environments are and logically separated from the production environment.	Inspected the separate development, QA and production environments to determine that development and test environments were 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.
		Back out procedures are documented to allow for rollback of application changes when changes impaired system operations.	Inspected the 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.
		A peer review is systematically required prior to deploying the PR into the production environment.	Inspected the supporting change ticket for a sample of infrastructure, database and application changes to determine that a peer review was systematically required prior to deploying the PR into the production environment.	No exceptions noted.
		Information security policies and procedures document the baseline requirements for configuration of IT systems and tools.	Inspected the information security policies and procedures to determine that information security policies and procedures documented the baseline requirements for configuration of IT systems and tools.	No exceptions noted.
		Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency situation.	Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in implementing changes in an emergency situation.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Risks identified as a part of the risk assessment process are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the risk assessment and management policies and procedures and completed risk assessment to determine that risks identified as a part of the risk assessment process were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
		Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	Inspected the risk assessment and management policies and procedures and completed risk assessment to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
		Documented policies and procedures are in place to guide personnel in performing risk assessment and risk mitigation activities.	Inspected the risk assessment and management policies and procedures to determine that documented policies and procedures were in place to guide personnel in performing risk assessment and risk mitigation activities.	No exceptions noted.
		The entity has purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	Inspected the insurance documentation to determine that the entity purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	No exceptions noted.

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

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 third-party attestation reports or vendor questionnaire for a sample of third-parties that the entity has a relationship with to determine that management obtained and reviewed attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Testing of the control activity disclosed that management did not obtain and review attestation reports and vendor questionnaires to evaluate the effectiveness of controls within the vendor or third-party's environment for three of five third-parties sampled.
		The entity has purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	Inspected the insurance documentation to determine that the entity purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	No exceptions noted.
		Management has defined a third-party vendor risk management process that specifies the process for evaluating third-party risks based on identified threats and the specified tolerances.	Inspected the vendor risk assessment policies and procedures to determine that management defined a third-party vendor risk management process that specified the process for evaluating third-party risks based on identified threats and the specified tolerances.	No exceptions noted.

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

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**
		A formal third-party risk assessment is performed on an annual basis to identify threats that could impair system commitments and requirements.	Inspected the vendor risk assessment policies and procedures to determine that a formal third-party risk assessment was performed on an annual basis to identify threats that could impair system commitments and requirements.	No exceptions noted.
		Management has assigned responsibility and accountability for the management of risks associated with third-parties to appropriate personnel.	Inspected the Director of Information Security job description to determine that management assigned responsibility and accountability for the management of risks associated with third-parties to appropriate personnel.	No exceptions noted.
		Management has established exception handling procedures for services provided by third-parties.	Inspected the third-party and vendor policies and procedures to determine that management established exception handling procedures for services provided by third-parties.	No exceptions noted.
		The entity has documented procedures for addressing issues identified with third-parties.	Inspected the third-party and vendor policies and procedures to determine that the entity documented procedures for addressing issues identified with third-parties.	No exceptions noted.
		The entity has documented procedures for terminating third-party relationships.	Inspected the third-party and vendor policies and procedures to determine that the entity documented procedures for terminating third-party relationships.	No exceptions noted.

SECTION 5

OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION

MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results	Management's Response
CC4.1, CC9.2	Management obtains and reviews attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Inspected the completed third-party attestation reports or vendor questionnaire for a sample of third-parties that the entity has a relationship with to determine that management obtained and reviewed attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Testing of the control activity disclosed that management did not obtain and review attestation reports and vendor questionnaires to evaluate the effectiveness of controls within the vendor or third-party's environment for three of five third-parties sampled.	During the review period, there was a transition in the CISO role, which caused a temporary lapse in the process of obtaining and reviewing attestation reports and vendor questionnaires for three of the five sampled vendors. The missing attestation reports and/or vendor questionnaires have now been received for all three vendors in question. A thorough review of these documents has been completed to evaluate the effectiveness of controls within each vendor's environment. Additionally, Mango Practice Management is now leveraging a third-party to manage their Information Security program, including vendor management.