SENTRY ASSURANCE

ALINE TECHNOLOGIES, INC.

SOC 2 Type 2

2026

REPORT ON ALINE TECHNOLOGIES, INC.'S DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATIONAL EFFECTIVENESS OF ITS CONTROLS RELEVANT TO COMMON CRITERIA/SECURITY

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

January 14, 2025 to January 13, 2026

TABLE OF CONTENTS

ASSERTION OF ALINE TECHNOLOGIES, INC. MANAGEMENT **4**

INDEPENDENT SERVICE AUDITOR'S REPORT **7**

ALINE TECHNOLOGIES, INC.'S DESCRIPTION OF ITS CONTRACT AUTOMATION AND MANAGEMENT SERVICES THROUGHOUT THE PERIOD JANUARY 14, 2025 TO JANUARY 13, 2026 ..... **12**

OVERVIEW OF OPERATIONS 13

Company Background *13*

Description of Services Provided *13*

Principal Service Commitments and System Requirements *13*

Components of the System *13*

BOUNDARIES OF THE SYSTEM 18

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING 18

Control Environment *18*

Risk Assessment Process *20*

Information and Communications Systems *20*

Monitoring Controls *21*

Changes to the System Since the Last Review *21*

Incidents Since the Last Review *21*

Trust Services Criteria Not Applicable to the System *21*

Subservice Organizations *21*

Subservice Description of Service *21*

Complementary Subservice Organization Controls *21*

COMPLEMENTARY USER ENTITY CONTROLS *23*

TRUST SERVICES CATEGORIES *23*

SECTION 4 INFORMATION PROVIDED BY THE SERVICE AUDITOR **24**

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR 25

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION 26

SECTION 5 OTHER INFORMATION PROVIDED BY MANAGEMENT **108**

SECTION 1
ASSERTION OF ALINE TECHNOLOGIES, INC. MANAGEMENT

ASSERTION OF ALINE TECHNOLOGIES, INC. MANAGEMENT

February 27, 2026

We have prepared the accompanying description of Aline Technologies, Inc.'s ('Aline' or 'service organization') Contract Automation and Management Services throughout the period January 14, 2025 to January 13, 2026 (description) based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022) in AICPA, Description Criteria (description criteria). The description is intended to provide report users with information about the Contract Automation and Management Services that may be useful when assessing the risks arising from interactions with Aline's system, particularly information about system controls that Aline 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 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022) in AICPA and Trust Services Criteria.

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

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

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

a. The description presents Aline's Contract Automation and Management Services system that was designed and implemented throughout the period January 14, 2025 to January 13, 2026, in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period January 14, 2025 to January 13, 2026 to provide reasonable assurance that Aline'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 Aline's controls throughout that period.
c. The controls stated in the description operated effectively throughout the period January 14, 2025 to January 13, 2026 to provide reasonable assurance that Aline's service commitments and system requirements would be achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of Aline's controls operated effectively throughout that period.
d. The following controls did not operate during the period January 14, 2025 to January 13, 2026, as the events that warrant the execution of the associated controls and processes did not occur:
    I. Personnel who violate information security policies are subject to disciplinary action and such disciplinary action is clearly documented in one or more policies.

II. New vendors are assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor. Reassessment occurs at least annually.
III. Vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis.
IV. A Data Retention and Disposal Policy specifies how customer data is to be retained and disposed of based on compliance requirements and contractual obligations.
V. Identified incidents are documented, tracked, and analyzed according to the Incident Response Plan.
VI. After any identified security incident has been resolved, management provides a "Lessons Learned" document to the team in order to continually improve security and operations.

Brent L. Farese

Brent Farese
Chief Executive Officer
Aline Technologies, Inc.

SECTION 2
INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Aline Technologies, Inc.

Scope

We have examined Aline's accompanying description of its Contract Automation and Management Services found in Section 3 titled Aline's Description of its Contract Automation and Management Services throughout the period January 14, 2025 to January 13, 2026 (description) based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022) in AICPA, Description Criteria, (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 14, 2025 to January 13, 2026, to provide reasonable assurance that Aline's service commitments and system requirements would be achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022) in AICPA and Trust Services Criteria.

Aline uses Amazon Web Services ('AWS') to provide Cloud Hosting Services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Aline, to achieve Aline's service commitments and system requirements based on the applicable trust services criteria. The description presents Aline's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Aline's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls .

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Aline, to achieve Aline's service commitments and system requirements based on the applicable trust services criteria . The description presents Aline's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Aline'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 V, "Other Information Provided by Management" is presented by the Company's management to provide additional information and is not a part of the Company's description made available to user entities during the period January 14, 2025 to January 13, 2026. Information within Section V, "Other Information Provided by Management" has not been subjected to the procedures applied in the examination and accordingly, we express no opinion on it.

Service Organization's Responsibilities

Aline 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 Aline's service commitments and system requirements would be achieved. In Section 1, Aline has provided the accompanying assertion titled Assertion of Aline Technologies, Inc. Management (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. Aline 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 AICPA. 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 would be 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 a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves—

- 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.
- 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 would achieve 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.

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 report users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design 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 Test of Controls

The specific controls we tested and the nature, timing, and results of those tests are presented in Section 4 of our report.

Aline Technologies, Inc.'s description of its System discussed the following controls that did not operate during the period January 14, 2025 to January 13, 2026, as the events that warrant the execution of the associated controls and processes did not occur:

- Personnel who violate information security policies are subject to disciplinary action and such disciplinary action is clearly documented in one or more policies.
- New vendors are assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor. Reassessment occurs at least annually.
- Vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis.
- A Data Retention and Disposal Policy specifies how customer data is to be retained and disposed of based on compliance requirements and contractual obligations.
- Identified incidents are documented, tracked, and analyzed according to the Incident Response Plan.
- After any identified security incident has been resolved, management provides a "Lessons Learned" document to the team in order to continually improve security and operations.

Opinion

In our opinion, in all material respects—

a. the description presents Aline's system that was designed and implemented throughout the period January 14, 2025 to January 13, 2026, in accordance with the description criteria.
b. the controls stated in the description were suitably designed and operating effectively throughout the period January 14, 2025 to January 13, 2026, to provide reasonable assurance that Aline'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 applied the complementary user entity controls assumed in the design of Aline's controls through that period.
c. the controls stated in the description operated effectively throughout the period January 14, 2025 to January 13, 2026 to provide reasonable assurance that Aline's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of Aline Technologies, Inc.'s controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4 of this report, is intended solely for the information and use of Aline; user entities of Aline's Contract Automation and Management Services system during some of or all of the period January 14, 2025 to January 13, 2026; business partners of Aline subject to risks arising from interactions with the Contract Automation and Management 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, and other parties.

- Internal control and its limitations.
- 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.

Sentry Assurance, LLC
Cleveland, Ohio
February 27, 2026

SECTION 3
ALINE TECHNOLOGIES, INC.'S DESCRIPTION OF ITS CONTRACT AUTOMATION AND MANAGEMENT SERVICES THROUGHOUT THE PERIOD JANUARY 14, 2025 TO JANUARY 13, 2026

OVERVIEW OF OPERATIONS

Company Background

Aline was founded in November 2019 with the objective of providing an AI contract lifecycle management platform.

The organization is based in New York, with workers remotely located in other areas of the United States and Canada.

As a B2B product, Aline serves broad industries including Legal Services, Real Estate services, Media companies, and many others.

Description of Services Provided

Aline provides contract lifecycle management (CLM) services primarily located in North America.

Aline's core application helps other companies manage their own contracts and other legal documents, supporting features such as:

- Drafting legal documents using Aline AI.
- Collaborating on legal documents in real time using Aline Editor.
- Negotiating contracts using AI features such as playbooks and AI assistant.
- Guiding an electronic signing process using AlineSign.
- Collecting signatures and other relevant information from users.
- Tracking other work around the legal document process.
- Reporting and summarizing existing/legacy legal documents in bulk using Aline AI Reports.
- Using Aline AI Associate as a legal agent to draft, negotiate, and analyze legal documents.

Principal Service Commitments and System Requirements

Aline Technologies, Inc. designs its processes and procedures to align with its objectives for its AI legal tech services. These objectives are based on service commitments made to clients, the regulatory landscape governing AI applications in legal contexts, and internal requirements for financial, operational, and compliance standards. Aline Technologies' services adhere to stringent security and privacy standards, including relevant state privacy laws across jurisdictions where it operates.

Security commitments to clients are formalized and communicated through Service Level Agreements (SLAs), customer contracts, and/or detailed descriptions of service offerings online. These commitments are standardized and encompass principles embedded within the core design of Aline's technology platform. These principles ensure that system users access information pertinent to their roles while preventing unauthorized access to sensitive data. Encryption technologies are deployed to safeguard customer data both in transit and at rest.

Aline Technologies establishes operational requirements that uphold its security commitments, regulatory obligations, and system specifications. These requirements are articulated in company policies, system design documentation, and contractual agreements with clients. Information security policies outline a comprehensive organizational approach to protecting systems and data, encompassing system design and development practices, operational procedures, network management protocols, and employee training and recruitment guidelines. Additionally, standard operating procedures detail the execution of manual and automated processes essential to the development and operation of Aline's AI legal tech platform.

Components of the System

The System description is comprised of the following components:

- Infrastructure – The collection of physical or virtual resources that supports an overall IT environment, including the physical environment and related structures, IT and hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile devices, and internal networks and connected external telecommunications networks) that the service organization used to provide the services.

- Software - The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external facing web applications, and the nature of applications developed in-house, including details about whether the applications in use mobile applications or desktop or laptop applications are.
- People - The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- Data – The types of data used by the system, such as transaction streams, files, databases, tables, and output used or processed by the system.
- Procedures – The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

Infrastructure

Primary Infrastructure	
Hardware	**Purpose**
AWS Cloud servers	All hosting, processing, and storage
Employee laptops (development)	Local repository and development tools
GitHub cloud servers	Code repository, continuous integration, security checks

Software

Primary Software	
Software	**Purpose**
Aline's custom built platform code	Aside from open-source libraries and vendor software, the entirety of the Aline's platform is proprietary
Slack	Internal organization communication
Google GSuite	Communication (internal and external)
Figma	Web design
Jira	Task management

People

Aline has a team which is actively growing as the company scales up, currently comprised of lawyers, full-stack software engineers, designers, marketers, sales professionals, and operational support for the foregoing. The company is led by a former Assistant General Counsel and a full-stack software engineer, Brent Farese (CEO), and an accomplished software engineer well-versed in AI, web development, and scalable infrastructure, Tim Buckley (CTO).

Data

Aline classifies data into four major categories:

- **Public:** Public data is information that may be disclosed to any person regardless of their affiliation with Aline Technologies, Inc. The Public classification is not limited to data that is of public interest or intended to be distributed to the public; the classification applies to data that does not require any level of protection from disclosure. While it may be necessary to protect

original (source) documents from unauthorized modification, Public data may be shared with a broad audience both within and outside Aline Technologies, Inc. and no steps need be taken to prevent its distribution. Public data can be retained for an indefinite period of time.

- **Internal:** Internal data is information that is potentially sensitive and is not intended to be shared with the public. Internal data should be classified as such when the unauthorized disclosure, alteration, or destruction of that data would result in moderate risk to Aline Technologies, Inc., its customers, or its partners. Internal data generally should not be disclosed outside of Aline Technologies, Inc. without the permission of the data owner. It is the responsibility of the data owner to designate information as Internal where appropriate. If you have questions about whether information is Internal or how to treat Internal data, you should talk to your manager or send an email to security@aline.co.
- **Confidential:** Confidential data is information that, if made available to unauthorized parties, may adversely affect individuals or Aline Technologies, Inc. This classification also includes data that Aline Technologies, Inc. may be required to keep confidential, either by law or under a confidentiality agreement with a third party, such as a vendor. This information should be protected against unauthorized disclosure or modification. Confidential data should be used only when necessary for business purposes and should be protected both when it is in use and when it is being stored or transported. Confidential data should be retained for only as long as it is needed to conduct internal/external business operations. Customer deletion requests and contractual deletion obligations should be the main source of authority for storing/deleting Confidential data.
- **Restricted:** Restricted data includes any information that Aline Technologies, Inc. has a legal or regulatory obligation to safeguard in the most stringent manner. Data should be classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to Aline Technologies, Inc., its customers, or its partners. The highest level of security controls should be applied to Restricted data.

Processes, Policies and Procedures

Aline management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorized by management. These procedures cover the following key security life cycle areas:

- Physical Security
- Logical Access
- Availability
- Change Control
- Data Communications
- Risk Assessment
- Data Retention
- Vendor Management

Physical Security

Aline's production servers are maintained by Amazon Web Services. The physical and environmental security protections are the responsibility of Amazon Web Services. Aline reviews the attestation reports and performs a risk analysis of Amazon Web Services' on at least an annual basis.

Logical Access

Aline employs a role-based security architecture, requiring system users to be identified and authenticated before accessing any resources. System protection is achieved through native security features and additional software products that authenticate users and validate access requests against authorized roles in access control lists. When incompatible responsibilities can't be segregated, Aline implements monitoring by either a superior without conflicting responsibilities or personnel from a separate department.

All resources are tracked in an asset inventory system, with each asset assigned an owner responsible for approving access and conducting periodic role-based access reviews.

Employees and approved vendors access Aline's network using secure credentials. Password policies, enforced through system settings, include account lockouts after failed attempts, and screen timeouts requiring re-authentication.

Remote access for employees requires token-based two-factor authentication. Tokens are issued upon employment and collected during exit interviews. Vendor personnel are not permitted remote access.

Customers access services via SSL-enabled web browsers, using valid credentials to access their cloud resources. Password requirements are configurable on virtual devices using the administration account. While Aline initially configures devices to its standards, these can be modified by the customer's virtual server administration account.

Customer employees may use virtual server administration accounts with two-factor, digital certificate-based authentication for system access.

New hire access is provisioned based on HR system reports, with pre-defined access rules based on roles. The security help desk creates user IDs and applies access rules accordingly.

Annual reviews of role-based access rules are conducted by a cross-functional team, with final approval from the CTO, who also reviews privileged access.

Daily termination reports from HR are used to delete access for departed employees. An annual active employee list is used to suspend and clear access for any missed terminations.

Quarterly manager reviews of employee roles are facilitated through the event management system. The security help desk processes changes and follows up on unreturned reviews. The CTO reviews and modifies privileged access as part of this process.

This comprehensive approach ensures appropriate, role-based access control, regular reviews, and timely access modifications at Aline.

Computer Operations – Backups

Customer data backup processes are closely monitored by operations personnel to ensure completion and identify any exceptions. If an exception occurs, the team conducts troubleshooting to determine the root cause. Depending on the customer's documented preferences, the backup job is either immediately re-run or scheduled for the next backup cycle.

The company takes physical security seriously, with backup infrastructure and on-site backup tape media securely stored in locked cabinets and/or caged environments within third-party data centers. Additionally, the backup infrastructure operates on private networks that are logically isolated from other networks to enhance security.

This comprehensive approach to data backup and storage ensures the security, availability, and recoverability of customer data while offering flexible options to meet varying customer needs.

Computer Operations – Availability

Aline has established incident response policies and procedures to guide staff in reporting and addressing information technology incidents. These procedures outline steps for identifying, reporting, and acting upon system security breaches and other incidents, with specific protocols in place for handling network-related issues.

The company closely monitors the capacity utilization of both internal and customer-facing physical and computing infrastructure to ensure service delivery aligns with agreed-upon service levels. Aline regularly

assesses the need for additional infrastructure capacity in response to existing customer growth or the onboarding of new clients. This infrastructure capacity monitoring encompasses various elements, including:

- CPU usage
- Memory usage
- Network bandwidth usage

Aline has implemented a robust patch management process to keep contracted customer and infrastructure systems up-to-date with vendor-recommended operating system patches. Both customers and Aline system owners review proposed patches to determine their applicability. The decision to apply patches is based on a risk assessment considering the security and availability impact on critical systems and applications. Aline's technical staff verify the successful installation of all approved patches and confirm any necessary system reboots have been completed.

This comprehensive approach allows Aline to maintain a secure, efficient, and scalable infrastructure while ensuring prompt response.

Change Control

Aline maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide staff in implementing and documenting application and infrastructure changes. These change control procedures cover change request and initiation processes, documentation requirements, development practices, quality assurance testing protocols, and necessary approval procedures.

The company uses a ticketing system to document change control procedures for application modifications and new implementations. Quality assurance testing and User Acceptance Testing (UAT) results are recorded and stored with their associated change requests. Development and testing occur in an environment logically separated from production. Management approval is required before changes are migrated to the production environment, with approvals documented within the ticketing system.

To maintain source code versions and facilitate migration through the development process to production, Aline employs version control software. This software maintains a history of code changes, enabling rollback capabilities and tracking changes to specific developers.

Aline has implemented a comprehensive patch management process to ensure that contracted customer and infrastructure systems receive vendor-recommended operating system patches. Both customers and Aline system owners review proposed patches to determine their applicability. The decision to apply patches is based on the security and availability impact on critical systems and applications. Aline staff verify that all approved patches have been installed and, if necessary, that system reboots have been completed.

This approach allows Aline to maintain a secure, up-to-date, and well-documented system environment while ensuring transparency and accountability in the change management process.

Data Communications

Aline employs firewall systems to filter unauthorized inbound network traffic from the Internet and block any network connections that aren't explicitly permitted. The company uses network address translation (NAT) to manage internal IP addresses. Only authorized employees have administrative access to the firewall.

The data center services are supported by a redundant system infrastructure to eliminate single points of failure, encompassing firewalls, routers, and servers. If a primary system fails, the redundant hardware is set up to take over seamlessly.

Aline engages a third-party vendor to conduct penetration testing, measuring the security posture of target systems or environments. The vendor follows an industry-standard methodology specified by Aline. This process begins with a vulnerability analysis, followed by attempts to exploit identified vulnerabilities, simulating either an insider threat or an external attacker who has gained internal network access. The testing covers network and application layers, as well as associated controls and processes, and is performed from both external and internal perspectives.

Quarterly vulnerability scanning is performed by another third-party vendor in line with Aline's policies. The vendor uses customized, industry-standard scanning technologies and follows a formal methodology specified by Aline. These scans are designed to efficiently test the organization's infrastructure and software while minimizing potential risks. Retests and on-demand scans are conducted as needed, typically during non-peak hours. Any tools requiring installation in Aline's system go through the Change Management process. Scans use approved templates and bandwidth-throttling options.

Authorized employees can access the system remotely via leading VPN technology. Employee authentication is secured through a token-based two-factor authentication system.

BOUNDARIES OF THE SYSTEM

The scope of this report includes the Contract Automation and Management Services performed in the Berkeley Heights, NJ facilities.

The scope of this report does not include the Cloud Hosting Services provided by Amazon Web Services performed in multiple facilities.

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

Control Environment

Integrity and Ethical Values

The efficacy of controls is inherently limited by the integrity and ethical standards of those who create, manage, and oversee them. Integrity and ethical values are fundamental to Aline's control environment, influencing the design, administration, and monitoring of all other components. These values are a product of Aline's ethical and behavioral standards, their communication methods, and how they're reinforced in practice. This includes leadership's efforts to eliminate or reduce incentives and temptations that might lead personnel to engage in dishonest, illegal, or unethical behavior. It also involves communicating organizational values and behavioral expectations to staff through policy statements, codes of conduct, and leading by example.

Aline has implemented specific control activities in this area, including:

- Formal, documented organizational policy statements and codes of conduct that clearly communicate company values and behavioral standards to all personnel.
- Policies requiring employees to sign acknowledgment forms confirming they've been granted access to the employee manual and understand their obligation to adhere to the policies and procedures it contains.
- A confidentiality clause in the employee handbook, which commits staff not to disclose proprietary or confidential information, including client data, to unauthorized parties.
- The inclusion of background checks as a standard component of the hiring process for all employes.

Commitment to Competence

At Aline, leadership views competence as the combination of knowledge and abilities essential for employees to fulfill their role-specific duties. The company's dedication to fostering competence involves evaluating the expertise required for various positions and determining how these requirements translate into specific skills and knowledge.

The organization has put in place targeted control measures in this domain, including:

- Leadership has assessed the competence levels needed for different roles and converted these requirements into documented job descriptions outlining necessary skills and knowledge.
  The company offers ongoing training to ensure that staff in particular positions maintain and enhance their skill sets.

Management's philosophy and operating style

The leadership approach and operational ethos at Aline encompass various aspects. These include how management assesses and oversees business risks, as well as their perspective on data processing, financial operations, and human resources.

In this area, the company has implemented specific control measures, such as:

- Regular briefings are provided to management on changes in regulations and industry trends that impact their service offerings.
- Top-level executives convene regularly to address significant initiatives and challenges affecting the entire organization.

Organizational Structure and Assignment of Authority and Responsibility

Aline's organizational framework serves as the foundation for planning, executing, controlling, and monitoring activities aimed at achieving company-wide goals. Leadership recognizes the importance of clearly defining key areas of authority and responsibility when establishing an effective organizational structure. The company has developed a structure tailored to its specific needs, taking into account its size and the nature of its operations.

The allocation of authority and responsibility at Aline encompasses various factors, including how operational duties are assigned and how reporting lines and approval hierarchies are structured. It also involves policies related to appropriate business practices, the expertise of key staff members, and the resources allocated for task completion. Furthermore, it includes guidelines and communications designed to ensure that employees understand the company's objectives, recognize how their individual efforts contribute to these goals, and are aware of their accountabilities.

Specific control measures implemented by Aline in this area include:

- The use of organizational charts to clearly illustrate key areas of authority and responsibility.
- Regular communication of these organizational charts to employees, with updates made as necessary to reflect any changes in the structure.

Human Resources Policies and Practices

Aline's success is built on a foundation of strong business ethics, complemented by high standards of efficiency, integrity, and ethical conduct. This success is reflected in the company's ability to attract and retain top-tier talent, ensuring optimal operational performance.

The company's approach to human resources encompasses a range of practices, including recruitment, onboarding, skill development, performance assessment, career guidance, advancement opportunities, compensation strategies, and disciplinary procedures.

Aline has implemented specific control measures in this domain, including:

- A requirement for all new hires to sign acknowledgment forms for the employee handbook and a confidentiality agreement during their first-day orientation.

- Annual performance evaluations conducted for every employee.
- Established employee exit procedures, documented in a comprehensive checklist, to guide the termination process when necessary.

Risk Assessment Process

The risk assessment approach at Aline identifies and addresses potential threats that could impact the company's ability to deliver dependable services to its clients. This continuous process requires leadership to pinpoint significant risks inherent in products or services within their areas of oversight. Aline's process involves identifying risk sources, evaluating their organizational impact, establishing acceptable risk thresholds, and implementing appropriate monitoring and management strategies.

Through this assessment, Aline has recognized risks stemming from its service offerings and has put measures in place to manage them. Key risk categories identified include:

- Operational risks: Arising from changes in the business environment, workforce, or leadership
- Strategic risks: Emerging from new technologies, evolving business models, and industry shifts
- Compliance risks: Related to changes in legal and regulatory landscapes

This approach aims to align Aline's strategy more closely with key stakeholders' interests, enhance organizational units' ability to manage uncertainty, minimize business threats, and capitalize on opportunities in a rapidly evolving market. Aline proactively works to identify and mitigate significant risks through various initiatives and maintains ongoing communication with leadership committees and top management.

Integration with Risk Assessment

The operational context of Aline's system, along with its commitments, agreements, and responsibilities, as well as the inherent nature of the system's components, all contribute to potential risks that could prevent the established criteria from being met. To address these risks, Aline implements carefully designed controls aimed at providing reasonable assurance that the criteria are fulfilled.

Given that each system and its operational environment are unique, the specific combination of risks threatening the criteria and the necessary controls to mitigate these risks will also be distinctive. As an integral part of the system's design and operation, Aline's leadership team identifies particular risks that could lead to unmet criteria and develops targeted controls to address these concerns.

The company recognizes that the interplay between the system, its environment, and potential risks creates a complex landscape that requires tailored solutions. By proactively identifying and addressing these unique challenges, Aline strives to maintain the integrity and effectiveness of its system in meeting established criteria.

Information and Communications Systems

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

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

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

Monitoring Controls

Aline's management continuously monitors controls to ensure they function as intended and adapts them as circumstances evolve. The leadership team conducts ongoing monitoring activities to assess the quality of internal control over time. When necessary, corrective measures are implemented to address any deviations from company policies and procedures. Employee activities and adherence to organizational guidelines are also closely observed.

On-Going Monitoring

Aline's management performs regular quality assurance checks, with additional training provided based on the outcomes of these monitoring procedures. These activities trigger corrective actions through departmental meetings, internal calls, and informal notifications.

The hands-on involvement of management in Aline's operations facilitates the identification of significant deviations from expected internal control performance. Senior leadership evaluates the specifics of any suspected control issues. Decisions on addressing control weaknesses are made based on whether the incident is isolated or necessitates changes in company procedures or staffing. This process aims to ensure legal compliance and optimize the performance of Aline's workforce.

Reporting Deficiencies

Aline employs an internal tracking system to document and monitor the results of ongoing monitoring procedures. Established escalation protocols ensure management is notified of any identified risks. High-priority risks receive immediate attention. When needed, corrective actions are documented and tracked within the internal system. Annual risk review meetings allow management to assess reported deficiencies and implement corrective measures.

Changes to the System Since the Last Review

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

Incidents Since the Last Review

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

Trust Services Criteria Not Applicable to the System

All Common Criteria/Security criterion were applicable to Aline's Contract Automation and Management Services system.

Subservice Organizations

This report does not include the Cloud Hosting Services provided by Amazon Web Services.

Subservice Description of Service

Amazon Web Services provides Cloud Hosting Services to support Aline Technologies, Inc.'s Contract Automation and Management Services.

Complementary Subservice Organization Controls

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

The following subservice organization controls should be implemented by Amazon Web Services and have not been included within the scope of this report.

Amazon Web Services		
Category	**Criteria**	**Control**
Security	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.
		Access to sensitive data center zones requires approval from authorized personnel and is controlled via badge access readers, biometric identification mechanism, and/or physical locks.
		Data center perimeters are defined and secured via physical barriers.
		Access lists to high security areas in data centers are reviewed on a defined basis and inappropriate access is removed in a timely manner.
		Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of the visit.
		Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.
		Data centers are continuously staffed and monitored by security personnel using real time video surveillance and/or alerts generated by security systems.
		The company reviews access to the data centers at least annually.
		The company has processes in place for granting, changing, and terminating physical access to company data centers based on an authorization from control owners.

Aline utilizes subservice organizations to provide certain components of its service. To ensure that the subservice organization controls are necessary, in combination with controls at Aline, to provide reasonable assurance that its service commitments and system requirements are achieved, Aline management defines the scope and responsibility of these controls through written contracts, such as service level agreements.

Aline conducts ongoing monitoring of the subservice organization controls, including the following procedures:

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

Aline documents the nature of the services provided by the subservice organization, relevant aspects of the subservice organization's infrastructure, software, people, procedures, and data, and the portions of the system that are attributable to the subservice organization when using the inclusive method. When

using the carve-out method, Aline documents the nature of the service provided by the subservice organization, each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, and the types of controls that service organization management assumed would be implemented by the subservice organization that are necessary, in combination with controls at Aline, to provide reasonable assurance that its service commitments and system requirements are achieved (complementary subservice organization controls or CSOCs).

COMPLEMENTARY USER ENTITY CONTROLS

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

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

1. User entities are responsible for understanding and complying with their contractual obligations to Aline.
2. User entities are responsible for notifying Aline of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record for content management.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Aline services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Aline's services.
6. User entities are responsible for providing Aline with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Aline of any actual or suspected information security breaches, including compromised user accounts used for integrations and file transfers.

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

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

SECTION 4

INFORMATION PROVIDED BY THE SERVICE AUDITOR

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

Sentry Assurance's examination of the controls of Aline was limited to the Trust Services Criteria, related criteria and control activities specified by the management of Aline and did not encompass all aspects of Aline'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 from service organization personnel. Inquiries were made to obtain information and representations from the client to determine 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	**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.	A Code of Conduct outlines ethical expectations, behavior standards, and ramifications of noncompliance.	Inspected the Code of Conduct to determine that a Code of Conduct outlined ethical expectations, behavior standards, and ramifications of noncompliance.	No Exceptions Noted
	An Internal Control Policy identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	Inspected the Internal Control Policy to determine that an internal Control Policy identified how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	No Exceptions Noted
	Internal personnel are evaluated via a formal performance review at least annually	Inspected the Performance Review Policy, the listing of current employees, and performance evaluation reports for a sample of employees to determine that internal personnel were evaluated via a formal performance review at least annually.	No Exceptions Noted
	Personnel who violate information security policies are subject to disciplinary action and such disciplinary action is clearly documented in one or more policies.	Inquired of management regarding disciplinary action processes for information security policy violations to determine that personnel who violated information security policies were subject to disciplinary action and such	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Control Environment			
CC1.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		disciplinary action was clearly documented in one or more policies.	
		Inspected the Code of Conduct to determine that personnel who violated information security policies were subject to disciplinary action and such disciplinary action was clearly documented in one or more policies.	No Exceptions Noted
		Disclosure Noted: Tests of the control activity disclosed that no disciplinary actions were taken within the review period, hence the operating effectiveness of the control cannot be determined.	Disclosure 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.	Senior management and/or board of directors meets at least quarterly to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least quarterly to discuss security risks, roles & responsibilities, controls, changes, audit results and/or other matters as necessary.	Inquired of management regarding senior leadership and information security meeting practices to determine that senior management and/or board of directors met at least quarterly to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters, and that the information security team met at least quarterly to discuss security risks, roles and responsibilities, controls,	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Control Environment			
CC1.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		changes, audit results and/or other matters as necessary.	
		Inspected the senior management meeting minutes for a sample of quarters to determine that senior management and/or board of directors met at least quarterly to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters, and that the information security team met at least quarterly to discuss security risks, roles and responsibilities, controls, changes, audit results and/or other matters as necessary.	No Exceptions Noted
	The board of directors or equivalent entity function includes senior management and external advisors, who are independent from the company's operations. An information security team has also been established to govern cybersecurity.	Inquired of management regarding the composition and structure of the board of directors and information security team to determine that the board of directors or equivalent entity function included senior management and external advisors, who were independent from The Company's operations, and that an information security team had been established to govern cybersecurity.	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Control Environment			
CC1.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Inspected the resumes for the independent members of the board of directors & the information security team to determine that the board of directors or equivalent entity function included senior management and external advisors, who were independent from the company's operations and an information security team had also been established to govern cybersecurity.	No Exceptions Noted
CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Management maintains a formal organizational chart to clearly identify positions of authority and the lines of communication, and publishes the organizational chart to internal personnel.	Inspected the organizational chart to determine that management maintains a formal organizational chart to clearly identify positions of authority and the lines of communication, and publishes the organizational chart to internal personnel.	No Exceptions Noted
	New vendors are assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor. Reassessment occurs at least annually.	Inquired of management regarding the vendor assessment and reassessment processes to determine that new vendors were assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor and that reassessment occurred at least annually.	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Control Environment			
CC1.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Inspected the Vendor Management Policy, the listing of vendors that were onboarded within the review period & current vendors, and the annual vendor reassessments for a sample of vendors to determine that new vendors were assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor and reassessment occurred at least annually.	No Exceptions Noted
		Disclosure Noted: Tests of the control activity disclosed that no new vendors within the review period, hence the operating effectiveness of the control cannot be determined.	Disclosure Noted
	Roles and responsibilities related to security for all personnel and executive roles are outlined in job descriptions and policies, as applicable	Inspected the Information Security Policy and a sample of job descriptions to determine that roles and responsibilities related to security for all personnel and executive roles were outlined in job descriptions and policies, as applicable	No Exceptions Noted
	Senior management and/or board of directors meets at least quarterly to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The	Inquired of management regarding senior leadership and information security meeting practices to determine that senior management	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Control Environment			
CC1.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	information security team meets at least quarterly to discuss security risks, roles & responsibilities, controls, changes, audit results and/or other matters as necessary.	and/or board of directors met at least quarterly to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters, and that the information security team met at least quarterly to discuss security risks, roles and responsibilities, controls, changes, audit results and/or other matters as necessary.	
		Inspected the senior management meeting minutes for a sample of quarters to determine that senior management and/or board of directors met at least quarterly to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters, and that the information security team met at least quarterly to discuss security risks, roles and responsibilities, controls, changes, audit results and/or other matters as necessary.	No Exceptions Noted
	The board of directors or equivalent entity function includes senior management and external advisors, who are independent from the company's operations.	Inquired of management regarding the composition and structure of the board of directors and information security team to determine that the board of	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Control Environment			
CC1.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	An information security team has also been established to govern cybersecurity.	directors or equivalent entity function included senior management and external advisors, who were independent from The Company's operations, and that an information security team had been established to govern cybersecurity.	
		Inspected the resumes for the independent members of the board of directors & the information security team to determine that the board of directors or equivalent entity function included senior management and external advisors, who were independent from the company's operations and an information security team had also been established to govern cybersecurity.	No Exceptions Noted
	Vendor SOC 2 reports (or equivalent) are collected and reviewed on at least an annual basis.	Inspected the Vendor Management Policy and the attestation reports vendor reviews for a sample of vendors to determine that vendor SOC 2 reports (or equivalent) were collected and reviewed on at least an annual basis.	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Control Environment			
CC1.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	A Code of Conduct outlines ethical expectations, behavior standards, and ramifications of noncompliance.	Inspected the Code of Conduct to determine that a Code of Conduct outlined ethical expectations, behavior standards, and ramifications of noncompliance.	No Exceptions Noted
	A Performance Review Policy provides personnel context and transparency into their performance and career development processes.	Inspected the Performance Review Policy to determine that a Performance Review Policy provided personnel context and transparency into their performance and career development processes.	No Exceptions Noted
	An Information Security Policy establishes the security requirements for maintaining the security, confidentiality, integrity, and availability of applications, systems, infrastructure, and data.	Inspected the Information Security Policy to determine that an Information Security Policy established the security requirements for maintaining the security, confidentiality, integrity, and availability of applications, systems, infrastructure, and data.	No Exceptions Noted
	An Internal Control Policy identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	Inspected the Internal Control Policy to determine that an internal Control Policy identified how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Control Environment			
CC1.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Background checks or their equivalent are performed before or promptly after a new hires start date, as permitted by local laws.	Inspected the Information Security Policy, the listing of contractors & employees that were onboarded within the review period, and background check reports for a sample of contractors & the total population of employees that were onboarded within the review period to determine that background checks or their equivalent were performed before or promptly after a new hires start date, as permitted by local laws.	No Exceptions Noted
	Hiring managers screen new hires or internal transfers to assess their qualifications, experience, and competency to fulfill their responsibilities. New hires sign confidentiality agreements or equivalents upon hire.	Inquired of management regarding the new hire and internal transfer screening processes to determine that hiring managers screened new hires or internal transfers to assess their qualifications, experience, and competency to fulfill their responsibilities and that new hires signed confidentiality agreements or equivalents upon hire.	No Exceptions Noted
		Inspected the Information Security Policy, the listing of employees that were onboarded within the review period, and confidentiality agreements & resumes for a sample of new hires to determine that hiring managers	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Control Environment			
CC1.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		screened new hires or internal transfers to assess their qualifications, experience, and competency to fulfill their responsibilities and that new hires signed confidentiality agreements or equivalents upon hire.	
	Internal personnel are evaluated via a formal performance review at least annually	Inspected the Performance Review Policy, the listing of current employees, and performance evaluation reports for a sample of employees to determine that internal personnel were evaluated via a formal performance review at least annually.	No Exceptions Noted
	Vendor SOC 2 reports (or equivalent) are collected and reviewed on at least an annual basis.	Inspected the Vendor Management Policy and the attestation reports & vendor reviews for a sample of vendors to determine that vendor SOC 2 reports (or equivalent) were collected and reviewed on at least an annual basis.	No Exceptions Noted
	Internal personnel complete annual training programs for information security to help them understand their obligations and responsibilities related to security.	Inquired of management regarding the policy acknowledgment process to determine that internal personnel reviewed and accepted applicable information security policies at least annually.	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Control Environment			
CC1.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Inspected the suite of information security policies, the listing of current internal personnel, and policy acknowledgments for a sample of internal personnel to determine that internal personnel review and accept applicable information security policies at least annually.	Exception noted. Reference Section V for further detail.
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	A Performance Review Policy provides personnel context and transparency into their performance and career development processes.	Inspected the Performance Review Policy to determine that a Performance Review Policy provided personnel context and transparency into their performance and career development processes.	No Exceptions Noted
	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Inspected the continuous monitoring solution dashboard to determine that a continuous monitoring solution monitored internal controls used in the achievement of service commitments and system requirements.	No Exceptions Noted
	An Internal Control Policy identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	Inspected the Internal Control Policy to determine that an internal Control Policy identified how a system of controls should be maintained to safeguard assets, promote operational	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Control Environment			
CC1.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		efficiency, and encourage adherence to prescribed managerial policies.	
	Internal personnel are evaluated via a formal performance review at least annually	Inspected the Performance Review Policy, the listing of current employees, and performance evaluation reports for a sample of employees to determine that internal personnel were evaluated via a formal performance review at least annually.	No Exceptions Noted
	Management maintains a formal organizational chart to clearly identify positions of authority and the lines of communication, and publishes the organizational chart to internal personnel.	Inspected the organizational chart to determine that management maintains a formal organizational chart to clearly identify positions of authority and the lines of communication, and publishes the organizational chart to internal personnel.	No Exceptions Noted
	Personnel who violate information security policies are subject to disciplinary action and such disciplinary action is clearly documented in one or more policies.	Inquired of management regarding disciplinary action processes for information security policy violations to determine that personnel who violated information security policies were subject to disciplinary action and such disciplinary action was clearly documented in one or more policies.	No Exceptions Noted
		Inspected the Code of Conduct to determine that personnel who violated	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Control Environment			
CC1.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		information security policies were subject to disciplinary action and such disciplinary action was clearly documented in one or more policies.	
		Disclosure Noted: Tests of the control activity disclosed that no disciplinary actions were taken within the review period, hence the operating effectiveness of the control cannot be determined.	Disclosure Noted
	Senior management and/or board of directors meets at least quarterly to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least quarterly to discuss security risks, roles & responsibilities, controls, changes, audit results and/or other matters as necessary.	Inquired of management regarding senior leadership and information security meeting practices to determine that senior management and/or board of directors met at least quarterly to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters, and that the information security team met at least quarterly to discuss security risks, roles and responsibilities, controls, changes, audit results and/or other matters as necessary.	No Exceptions Noted
		Inspected the senior management meeting minutes for a sample of quarters to determine that senior	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Control Environment			
CC1.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		management and/or board of directors met at least quarterly to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters, and that the information security team met at least quarterly to discuss security risks, roles and responsibilities, controls, changes, audit results and/or other matters as necessary.	

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Information and Communication			
CC2.0	**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.	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Inspected the continuous monitoring solution dashboard to determine that a continuous monitoring solution monitored internal controls used in the achievement of service commitments and system requirements.	No Exceptions Noted
	A third party is engaged to conduct a network and application penetration test of the production environment at least annually. Critical and high-risk findings are tracked through resolution.	Inquired of management regarding penetration testing practices and remediation processes to determine that a third party was engaged to conduct a network and application penetration test of the production environment at least annually and that critical and high-risk findings were tracked through resolution.	No Exceptions Noted
		Inspected the Vulnerability Management Policy, penetration test statement of work, and penetration test scoping documentation to determine that a third party was engaged to conduct a network and application penetration test of the production environment at least annually and critical and high-risk findings were tracked through resolution.	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Information and Communication			
CC2.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	An Information Security Policy establishes the security requirements for maintaining the security, confidentiality, integrity, and availability of applications, systems, infrastructure, and data.	Inspected the Information Security Policy to determine that an Information Security Policy established the security requirements for maintaining the security, confidentiality, integrity, and availability of applications, systems, infrastructure, and data.	No Exceptions Noted
	Formal risk assessments are performed, which includes the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Inspected the Risk Assessment & Treatment Policy and the annual risk assessment report to determine that formal risk assessments were performed, which included the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	No Exceptions Noted
	Vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis.	Inquired of management regarding vulnerability scanning practices and remediation processes to determine that vulnerability scanning was performed on production infrastructure systems, and identified deficiencies were remediated on a timely basis.	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Information and Communication			
CC2.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Inspected the Vulnerability & Patch Management Policy, the listing of vulnerabilities identified during host based & dependency scans, and remediation tickets for a sample of vulnerabilities identified during dependency scanning to determine that vulnerability scanning was performed on production infrastructure systems, and identified deficiencies were remediated on a timely basis.	No Exceptions Noted
		Disclosure Noted: Tests of the control activity disclosed that no critical or high vulnerabilities were identified during host-based vulnerability scans within the review period, hence the operating effectiveness of the control cannot be determined.	Disclosure Noted
CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and	A Network Security Policy identifies the requirements for protecting information and systems within and across networks.	Inspected the Network Security Policy to determine that a Network Security Policy identified the requirements for protecting information and systems within and across networks.	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Information and Communication			
CC2.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
responsibilities for internal control, necessary to support the functioning of internal control.	A reporting channel is made available to internal personnel and external parties to report security and other identified concerns.	Inspected the internal reporting channel and the Privacy Policy to determine that a reporting channel was made available to internal personnel and external parties to report security and other identified concerns.	No Exceptions Noted
	An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution.	Inspected the Security Incident Response Plan to determine that the company had an Incident Response Plan that outlined the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution.	No Exceptions Noted
	An infrastructure architecture and network diagram is maintained.	Inspected the architectural diagram to determine that an infrastructure architecture and network diagram was maintained.	No Exceptions Noted
	Descriptions of the company's services and systems are available to both internal personnel and external users.	Inspected the system and service descriptions available to internal personnel and external users to determine that descriptions of the company's services and systems were available to both internal personnel and external users.	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Information and Communication			
CC2.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Roles and responsibilities related to security for all personnel and executive roles are outlined in job descriptions and policies, as applicable	Inspected the Information Security Policy and a sample of job descriptions to determine that roles and responsibilities related to security for all personnel and executive roles were outlined in job descriptions and policies, as applicable	No Exceptions Noted
	Senior management and/or board of directors meets at least quarterly to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least quarterly to discuss security risks, roles & responsibilities, controls, changes, audit results and/or other matters as necessary.	Inquired of management regarding senior leadership and information security meeting practices to determine that senior management and/or board of directors met at least quarterly to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters, and that the information security team met at least quarterly to discuss security risks, roles and responsibilities, controls, changes, audit results and/or other matters as necessary.	No Exceptions Noted
		Inspected the senior management meeting minutes for a sample of quarters to determine that senior management and/or board of directors met at least quarterly to review business goals, company initiatives, resource needs, risk management	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Information and Communication			
CC2.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		activities, and other internal/external matters, and that the information security team met at least quarterly to discuss security risks, roles and responsibilities, controls, changes, audit results and/or other matters as necessary.	
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	A Privacy Policy is established to external users describing the company's privacy commitments.	Inspected the publicly available Privacy Policy to determine that a Privacy Policy was established to external users describing the company's privacy commitments.	No Exceptions Noted
	A reporting channel is made available to internal personnel and external parties to report security and other identified concerns.	Inspected the internal reporting channel and the Privacy Policy to determine that a reporting channel was made available to internal personnel and external parties to report security and other identified concerns.	No Exceptions Noted
	An infrastructure architecture and network diagram is maintained.	Inspected the architectural diagram to determine that an infrastructure architecture and network diagram was maintained.	No Exceptions Noted
	Critical information is communicated to external parties, as applicable.	Inspected the Terms of Service, the application status page, and a sample of change notifications to determine that critical information was	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Information and Communication			
CC2.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		communicated to external parties, as applicable.	
	Descriptions of the company's services and systems are available to both internal personnel and external users.	Inspected the system and service descriptions available to internal personnel and external users to determine that descriptions of the company's services and systems were available to both internal personnel and external users.	No Exceptions Noted
	New vendors are assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor. Reassessment occurs at least annually.	Inquired of management regarding the vendor assessment and reassessment processes to determine that new vendors were assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor and that reassessment occurred at least annually.	No Exceptions Noted
		Inspected the Vendor Management Policy, the listing of vendors that were onboarded within the review period & current vendors, and the annual vendor reassessments for a sample of vendors to determine that new vendors were assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor and	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Information and Communication			
CC2.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		reassessment occurred at least annually.	
		Disclosure Noted: Tests of the control activity disclosed that no new vendors within the review period, hence the operating effectiveness of the control cannot be determined.	Disclosure Noted
	Security commitments and expectations are communicated to both internal personnel and external users via the company's website.	Inspected the publicly available Privacy Policy & Terms of Service to determine that security commitments and expectations were communicated to both internal personnel and external users via the Company's website.	No Exceptions Noted
	Senior management and/or board of directors meets at least quarterly to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least quarterly to discuss security risks, roles & responsibilities, controls, changes, audit results and/or other matters as necessary.	Inquired of management regarding senior leadership and information security meeting practices to determine that senior management and/or board of directors met at least quarterly to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters, and that the information security team met at least quarterly to discuss security risks, roles and responsibilities, controls,	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Information and Communication			
CC2.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		changes, audit results and/or other matters as necessary.	
		Inspected the senior management meeting minutes for a sample of quarters to determine that senior management and/or board of directors met at least quarterly to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters, and that the information security team met at least quarterly to discuss security risks, roles and responsibilities, controls, changes, audit results and/or other matters as necessary.	No Exceptions Noted
	Internal personnel complete annual training programs for information security to help them understand their obligations and responsibilities related to security.	Inquired of management regarding the policy acknowledgment process to determine that internal personnel reviewed and accepted applicable information security policies at least annually.	No Exceptions Noted
		Inspected the suite of information security policies, the listing of current internal personnel, and policy acknowledgments for a sample of internal personnel to determine that	Exception noted. Reference Section

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Information and Communication			
CC2.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		internal personnel review and accept applicable information security policies at least annually.	V for further detail.
	Terms of Service or the equivalent are published or shared to external users.	Inspected the publicly available Terms of Service to determine that Terms of Service or the equivalent were published or shared to external users.	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Risk Assessment			
CC3.0	**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.	A Risk Assessment and Treatment Policy governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners. Risk tolerance and strategies are also defined in the policy.	Inspected the Risk Assessment and Treatment Policy to determine that a Risk Assessment and Treatment Policy governed the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners, and that risk tolerance and strategies were also defined in the policy.	No Exceptions Noted
	Formal risk assessments are performed, which includes the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Inspected the Risk Assessment & Treatment Policy and the annual risk assessment report to determine that formal risk assessments were performed, which included the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	No Exceptions Noted
	Senior management and/or board of directors meets at least quarterly to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least quarterly to discuss security risks, roles & responsibilities,	Inquired of management regarding senior leadership and information security meeting practices to determine that senior management and/or board of directors met at least quarterly to review business goals, company initiatives, resource needs,	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Risk Assessment			
CC3.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	controls, changes, audit results and/or other matters as necessary.	risk management activities, and other internal/external matters, and that the information security team met at least quarterly to discuss security risks, roles and responsibilities, controls, changes, audit results and/or other matters as necessary.	
		Inspected the senior management meeting minutes for a sample of quarters to determine that senior management and/or board of directors met at least quarterly to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters, and that the information security team met at least quarterly to discuss security risks, roles and responsibilities, controls, changes, audit results and/or other matters as necessary.	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	A Risk Assessment and Treatment Policy governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners. Risk tolerance and strategies are also defined in the policy.	Inspected the Risk Assessment and Treatment Policy to determine that a Risk Assessment and Treatment Policy governed the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Risk Assessment			
CC3.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
determining how the risks should be managed.		members, customers, vendors, suppliers, and partners, and that risk tolerance and strategies were also defined in the policy.	
	A risk register is maintained, which records the risk mitigation strategies for identified risks, and the development or modification of controls consistent with the risk mitigation strategy.	Inspected the Risk Assessment & Treatment Policy and the annual risk assessment report to determine that a risk register was maintained, which recorded the risk mitigation strategies for identified risks, and the development or modification of controls consistent with the risk mitigation strategy.	No Exceptions Noted
	Formal risk assessments are performed, which includes the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Inspected the Risk Assessment & Treatment Policy and the annual risk assessment report to determine that formal risk assessments were performed, which included the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	No Exceptions Noted
	New vendors are assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor. Reassessment occurs at least annually.	Inquired of management regarding the vendor assessment and reassessment processes to determine that new vendors were assessed in accordance	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Risk Assessment			
CC3.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		with the Vendor Risk Management Policy prior to engaging with the vendor and that reassessment occurred at least annually.	
		Inspected the Vendor Management Policy, the listing of vendors that were onboarded within the review period & current vendors, and the annual vendor reassessments for a sample of vendors to determine that new vendors were assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor and reassessment occurred at least annually.	No Exceptions Noted
		Disclosure Noted: Tests of the control activity disclosed that no new vendors within the review period, hence the operating effectiveness of the control cannot be determined.	Disclosure Noted
	Vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis.	Inquired of management regarding vulnerability scanning practices and remediation processes to determine that vulnerability scanning was performed on production infrastructure systems, and identified	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Risk Assessment			
CC3.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		deficiencies were remediated on a timely basis.	
		Inspected the Vulnerability & Patch Management Policy, the listing of vulnerabilities identified during host based & dependency scans, and remediation tickets for a sample of vulnerabilities identified during dependency scanning to determine that vulnerability scanning was performed on production infrastructure systems, and identified deficiencies were remediated on a timely basis.	No Exceptions Noted
		Disclosure Noted: Tests of the control activity disclosed that no critical or high vulnerabilities were identified during host-based vulnerability scans within the review period, hence the operating effectiveness of the control cannot be determined.	Disclosure Noted
CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the	Formal risk assessments are performed, which includes the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Inspected the Risk Assessment & Treatment Policy and the annual risk assessment report to determine that formal risk assessments were performed, which included the identification of relevant internal and	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Risk Assessment			
CC3.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
achievement of objectives.		external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Formal risk assessments are performed, which includes the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Inspected the Risk Assessment & Treatment Policy and the annual risk assessment report to determine that formal risk assessments were performed, which included the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	No Exceptions Noted
	New vendors are assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor. Reassessment occurs at least annually.	Inquired of management regarding the vendor assessment and reassessment processes to determine that new vendors were assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor and that reassessment occurred at least annually.	No Exceptions Noted
		Inspected the Vendor Management Policy, the listing of vendors that were onboarded within the review period & current vendors, and the annual vendor reassessments for a sample of vendors	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Risk Assessment			
CC3.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		to determine that new vendors were assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor and reassessment occurred at least annually.	
		Disclosure Noted: Tests of the control activity disclosed that no new vendors within the review period, hence the operating effectiveness of the control cannot be determined.	Disclosure Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Monitoring Activities			
CC4.0	**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.	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Inspected the continuous monitoring solution dashboard to determine that a continuous monitoring solution monitored internal controls used in the achievement of service commitments and system requirements.	No Exceptions Noted
	A third party is engaged to conduct a network and application penetration test of the production environment at least annually. Critical and high-risk findings are tracked through resolution.	Inquired of management regarding penetration testing practices and remediation processes to determine that a third party was engaged to conduct a network and application penetration test of the production environment at least annually and that critical and high-risk findings were tracked through resolution.	No Exceptions Noted
		Inspected the Vulnerability Management Policy, penetration test statement of work, and penetration test scoping documentation to determine that a third party was engaged to conduct a network and application penetration test of the production environment at least annually and critical and high-risk findings were tracked through resolution.	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Monitoring Activities			
CC4.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	An Internal Control Policy identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	Inspected the Internal Control Policy to determine that an internal Control Policy identified how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	No Exceptions Noted
	Vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis.	Inquired of management regarding vulnerability scanning practices and remediation processes to determine that vulnerability scanning was performed on production infrastructure systems, and identified deficiencies were remediated on a timely basis.	No Exceptions Noted
		Inspected the Vulnerability & Patch Management Policy, the listing of vulnerabilities identified during host based & dependency scans, and remediation tickets for a sample of vulnerabilities identified during dependency scanning to determine that vulnerability scanning was performed on production infrastructure systems, and identified deficiencies were remediated on a timely basis.	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Monitoring Activities			
CC4.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Disclosure Noted: Tests of the control activity disclosed that no critical or high vulnerabilities were identified during host-based vulnerability scans within the review period, hence the operating effectiveness of the control cannot be determined.	Disclosure Noted
CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Inspected the continuous monitoring solution dashboard to determine that a continuous monitoring solution monitored internal controls used in the achievement of service commitments and system requirements.	No Exceptions Noted
	A third party is engaged to conduct a network and application penetration test of the production environment at least annually. Critical and high-risk findings are tracked through resolution.	Inquired of management regarding penetration testing practices and remediation processes to determine that a third party was engaged to conduct a network and application penetration test of the production environment at least annually and that critical and high-risk findings were tracked through resolution.	No Exceptions Noted
		Inspected the Vulnerability Management Policy, penetration test statement of work, and penetration test scoping documentation to determine that a third party was	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Monitoring Activities			
CC4.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		engaged to conduct a network and application penetration test of the production environment at least annually and critical and high-risk findings were tracked through resolution.	
	Senior management and/or board of directors meets at least quarterly to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least quarterly to discuss security risks, roles & responsibilities, controls, changes, audit results and/or other matters as necessary.	Inquired of management regarding senior leadership and information security meeting practices to determine that senior management and/or board of directors met at least quarterly to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters, and that the information security team met at least quarterly to discuss security risks, roles and responsibilities, controls, changes, audit results and/or other matters as necessary.	No Exceptions Noted
		Inspected the senior management meeting minutes for a sample of quarters to determine that senior management and/or board of directors met at least quarterly to review business goals, company initiatives, resource needs, risk management activities, and other internal/external	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Monitoring Activities			
CC4.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		matters, and that the information security team met at least quarterly to discuss security risks, roles and responsibilities, controls, changes, audit results and/or other matters as necessary.	
	Vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis.	Inquired of management regarding vulnerability scanning practices and remediation processes to determine that vulnerability scanning was performed on production infrastructure systems, and identified deficiencies were remediated on a timely basis.	No Exceptions Noted
		Inspected the Vulnerability & Patch Management Policy, the listing of vulnerabilities identified during host based & dependency scans, and remediation tickets for a sample of vulnerabilities identified during dependency scanning to determine that vulnerability scanning was performed on production infrastructure systems, and identified deficiencies were remediated on a timely basis.	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Monitoring Activities			
CC4.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Disclosure Noted: Tests of the control activity disclosed that no critical or high vulnerabilities were identified during host-based vulnerability scans within the review period, hence the operating effectiveness of the control cannot be determined.	Disclosure Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Control Activities			
CC5.0	**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.	A Vendor Risk Management Policy defines a framework for the onboarding and management of the vendor relationship lifecycle.	Inspected the Vendor Management Policy to determine that a Vendor Risk Management Policy defined a framework for the onboarding and management of the vendor relationship lifecycle.	No Exceptions Noted
	An Internal Control Policy identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	Inspected the Internal Control Policy to determine that an internal Control Policy identified how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	No Exceptions Noted
	Formal risk assessments are performed, which includes the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Inspected the Risk Assessment & Treatment Policy and the annual risk assessment report to determine that formal risk assessments were performed, which included the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	No Exceptions Noted
CC5.2 - COSO Principle 11: The entity also selects and develops	A Secure Development Policy defines the requirements for secure software and system development and maintenance.	Inspected the Secure Development Policy to determine that a Secure Development Policy defined the	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Control Activities			
CC5.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
general control activities over technology to support the achievement of objectives.		requirements for secure software and system development and maintenance.	
	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Inspected the continuous monitoring solution dashboard to determine that a continuous monitoring solution monitored internal controls used in the achievement of service commitments and system requirements.	No Exceptions Noted
	An Internal Control Policy identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	Inspected the Internal Control Policy to determine that an internal Control Policy identified how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	No Exceptions Noted
	Roles and responsibilities related to security for all personnel and executive roles are outlined in job descriptions and policies, as applicable	Inspected the Information Security Policy and a sample of job descriptions to determine that roles and responsibilities related to security for all personnel and executive roles were outlined in job descriptions and policies, as applicable	No Exceptions Noted
CC5.3 - COSO Principle 12: The entity deploys control activities through policies that	A Change Management Policy governs the documenting, tracking, testing, and approving of system, network, security, and infrastructure changes.	Inspected the Change Management Policy to determine that a Change Management Policy governed the documenting, tracking, testing, and	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Control Activities			
CC5.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
establish what is expected and in procedures that put policies into action.		approving of system, network, security, and infrastructure changes.	
	A Configuration and Asset Management Policy governs configurations for new sensitive systems.	Inspected the Configuration and Asset Management Policy to determine that a Configuration and Asset Management Policy governed configurations for new sensitive systems.	No Exceptions Noted
	A Data Classification Policy details the security and handling protocols for sensitive data.	Inspected the Data Classification Policy to determine that a Data Classification Policy detailed the security and handling protocols for sensitive data.	No Exceptions Noted
	A Data Retention and Disposal Policy specifies how customer data is to be retained and disposed of based on compliance requirements and contractual obligations.	Inquired of management regarding data retention and disposal practices to determine that a Data Retention and Disposal Policy specified how customer data was to be retained and disposed of based on compliance requirements and contractual obligations.	No Exceptions Noted
		Inspected the Data Retention & Disposal Policy and the listing of data disposals due to retention guidelines within the review period to determine that a Data Retention and Disposal Policy specified how customer data was to be retained and disposed of	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Control Activities			
CC5.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		based on compliance requirements and contractual obligations.	
		Disclosure Noted: Tests of the control activity disclosed that no data disposals due to retention guidelines occurred within the review period, hence the operating effectiveness of the control cannot be determined.	Disclosure Noted
	A Network Security Policy identifies the requirements for protecting information and systems within and across networks.	Inspected the Network Security Policy to determine that a Network Security Policy identified the requirements for protecting information and systems within and across networks.	No Exceptions Noted
	A Performance Review Policy provides personnel context and transparency into their performance and career development processes.	Inspected the Performance Review Policy to determine that a Performance Review Policy provided personnel context and transparency into their performance and career development processes.	No Exceptions Noted
	A Privacy Policy is established to external users describing the company's privacy commitments.	Inspected the publicly available Privacy Policy to determine that a Privacy Policy was established to external users describing the company's privacy commitments.	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Control Activities			
CC5.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	A Risk Assessment and Treatment Policy governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners. Risk tolerance and strategies are also defined in the policy.	Inspected the Risk Assessment and Treatment Policy to determine that a Risk Assessment and Treatment Policy governed the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners, and that risk tolerance and strategies were also defined in the policy.	No Exceptions Noted
	A Secure Development Policy defines the requirements for secure software and system development and maintenance.	Inspected the Secure Development Policy to determine that a Secure Development Policy defined the requirements for secure software and system development and maintenance.	No Exceptions Noted
	A Vendor Risk Management Policy defines a framework for the onboarding and management of the vendor relationship lifecycle.	Inspected the Vendor Management Policy to determine that a Vendor Risk Management Policy defined a framework for the onboarding and management of the vendor relationship lifecycle.	No Exceptions Noted
	A Vulnerability Management and Patch Management Policy outlines the processes to efficiently respond to identified vulnerabilities.	Inspected the Vulnerability Management and Patch Management Policy to determine that a Vulnerability Management and Patch Management Policy outlined the processes to	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Control Activities			
CC5.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		efficiently respond to identified vulnerabilities.	
	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Inspected the continuous monitoring solution dashboard to determine that a continuous monitoring solution monitored internal controls used in the achievement of service commitments and system requirements.	No Exceptions Noted
	An Acceptable Use Policy defines standards for appropriate and secure use of company hardware and electronic systems including storage media, communication tools and internet access.	Inspected the Acceptable Use Policy to determine that an Acceptable Use Policy defined standards for appropriate and secure use of company hardware and electronic systems including storage media, communication tools and internet access.	No Exceptions Noted
	An Access Control and Termination Policy governs authentication and access to applicable systems, data, and networks.	Inspected the Access Control & Termination Policy to determine that an Access Control and Termination Policy governed authentication and access to applicable systems, data, and networks.	No Exceptions Noted
	An Encryption and Key Management Policy supports the secure encryption and decryption of app secrets, and governs the use of cryptographic controls.	Inspected the Encryption and Key Management Policy to determine that an Encryption and Key Management Policy supported the secure encryption	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Control Activities			
CC5.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		and decryption of app secrets, and governs the use of cryptographic controls.	
	An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution.	Inspected the Security Incident Response Plan to determine that the company had an Incident Response Plan that outlined the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution.	No Exceptions Noted
	An Information Security Policy establishes the security requirements for maintaining the security, confidentiality, integrity, and availability of applications, systems, infrastructure, and data.	Inspected the Information Security Policy to determine that an Information Security Policy established the security requirements for maintaining the security, confidentiality, integrity, and availability of applications, systems, infrastructure, and data.	No Exceptions Noted
	An Internal Control Policy identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	Inspected the Internal Control Policy to determine that an internal Control Policy identified how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	No Exceptions Noted
	Business Continuity and Disaster Recovery Policy governs required processes for restoring the service	Inspected the Business Continuity and Disaster Recovery Policy to determine	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Control Activities			
CC5.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	or supporting infrastructure after suffering a disaster or disruption.	that business Continuity and Disaster Recovery Policy governed required processes for restoring the service or supporting infrastructure after suffering a disaster or disruption.	
	Internal personnel review and accept applicable information security policies at least annually.	Inquired of management regarding the policy acknowledgment process to determine that internal personnel reviewed and accepted applicable information security policies at least annually.	No Exceptions Noted
		Inspected the suite of information security policies, the listing of current internal personnel, and policy acknowledgments for a sample of internal personnel to determine that internal personnel review and accept applicable information security policies at least annually.	Exception noted. Reference Section V for further detail.
	Management is responsible for the design, implementation, and management of the organization's security policies and procedures. The policies and procedures are reviewed by management at least annually.	Inspected the suite of policies and the review history to determine that policies and procedures were reviewed and updated by management at least annually.	No Exceptions Noted
	Personnel who violate information security policies are subject to disciplinary action and such	Inquired of management regarding disciplinary action processes for	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Control Activities			
CC5.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	disciplinary action is clearly documented in one or more policies.	information security policy violations to determine that personnel who violated information security policies were subject to disciplinary action and such disciplinary action was clearly documented in one or more policies.	
		Inspected the Code of Conduct to determine that personnel who violated information security policies were subject to disciplinary action and such disciplinary action was clearly documented in one or more policies.	No Exceptions Noted
		Disclosure Noted: Tests of the control activity disclosed that no disciplinary actions were taken within the review period, hence the operating effectiveness of the control cannot be determined.	Disclosure Noted
	Roles and responsibilities related to security for all personnel and executive roles are outlined in job descriptions and policies, as applicable	Inspected the Information Security Policy and a sample of job descriptions to determine that roles and responsibilities related to security for all personnel and executive roles were outlined in job descriptions and policies, as applicable	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Logical and Physical Access			
CC6.0	**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.	A Configuration and Asset Management Policy governs configurations for new sensitive systems.	Inspected the Configuration and Asset Management Policy to determine that a Configuration and Asset Management Policy governed configurations for new sensitive systems.	No Exceptions Noted
	A list of system assets, components, and respective owners are maintained and reviewed at least annually.	Inquired of management regarding the asset inventory process to determine that a list of system assets, components, and respective owners was maintained and reviewed at least annually.	No Exceptions Noted
		Inspected the Configuration & Asset Management Policy and the physical & cloud asset inventories to determine that a list of system assets, components, and respective owners was maintained and reviewed at least annually.	No Exceptions Noted
	An Access Control and Termination Policy governs authentication and access to applicable systems, data, and networks.	Inspected the Access Control & Termination Policy to determine that an Access Control and Termination Policy governed authentication and access to applicable systems, data, and networks.	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Logical and Physical Access			
CC6.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	An Encryption and Key Management Policy supports the secure encryption and decryption of app secrets, and governs the use of cryptographic controls.	Inspected the Encryption and Key Management Policy to determine that an Encryption and Key Management Policy supported the secure encryption and decryption of app secrets, and governs the use of cryptographic controls.	No Exceptions Noted
	Company endpoints are managed and configured with anti-virus and hard drive encryption.	Inquired of management regarding endpoint security configurations to determine that Company endpoints were managed and configured with anti-virus and hard drive encryption.	No Exceptions Noted
		Inspected the Configuration & Asset Management Policy and the centralized encryption & anti-virus configurations for company owned workstations to determine that company endpoints were managed and configured with anti-virus and hard drive encryption.	No Exceptions Noted
	Configurations ensure available networking ports, protocols, services, and environments are restricted as necessary, including firewalls.	Inquired of management regarding firewall configurations and network security measures to determine that configurations ensured available networking ports, protocols, services, and environments were restricted as necessary, including firewalls.	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Logical and Physical Access			
CC6.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Observed the firewall and network configurations to determine that configurations ensured available networking ports, protocols, services, and environments were restricted as necessary, including firewalls.	No Exceptions Noted
		Inspected the Network Security Policy and the firewall configurations to determine that configurations ensured available networking ports, protocols, services, and environments were restricted as necessary, including firewalls.	No Exceptions Noted
	Personnel are assigned unique IDs to access sensitive systems, networks, and information	Inspected the Access Control & Termination Policy and the user listings for the application, codebase, database, network, and operating system to determine that personnel were assigned unique IDs to access sensitive systems, networks, and information	No Exceptions Noted
	Personnel are required to use strong, complex passwords and a second form of authentication to access sensitive systems, networks, and information.	Inspected the Access Control & Termination Policy and the password & multi-factor authentication (MFA) configurations for the application, codebase, database, network, & operating system to determine that	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Logical and Physical Access			
CC6.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		personnel were required to use strong, complex passwords and a second form of authentication to access sensitive systems, networks, and information.	
	Service data is encrypted at rest.	Inspected the Encryption & Key Management Policy and the database encryption configurations to determine that service data was encrypted at rest.	No Exceptions Noted
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Administrative access to production infrastructure is restricted based on the principle of least privilege.	Inquired of management regarding administrative access measures and permissions to production infrastructure to determine that administrative access to production infrastructure was restricted based on the principle of least privilege.	No Exceptions Noted
		Inspected the Access Control & Termination Policy, the administrator listings for the application, codebase, database, network, & operating system, and the administrator privileges for the application, database, and operating system to determine that administrative access to production infrastructure was restricted based on the principle of least privilege.	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Logical and Physical Access			
CC6.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	An Access Control and Termination Policy governs authentication and access to applicable systems, data, and networks.	Inspected the Access Control & Termination Policy to determine that an Access Control and Termination Policy governed authentication and access to applicable systems, data, and networks.	No Exceptions Noted
	System owners conduct scheduled user access reviews of production servers, databases, and applications to validate internal user access is commensurate with job responsibilities.	Inquired of management regarding the user access review process to determine that system owners conducted scheduled user access reviews of production servers, databases, and applications to validate internal user access was commensurate with job responsibilities.	No Exceptions Noted
		Inspected the Access Control & Termination Policy and a sample bi-annual user access review report to determine that system owners conducted scheduled user access reviews of production servers, databases, and applications to validate internal user access was commensurate with job responsibilities.	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Logical and Physical Access			
CC6.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Upon termination or when internal personnel no longer require access, system access is removed, as applicable.	Inquired of management regarding the access removal and termination process to determine that upon termination or when internal personnel no longer required access, system access was removed, as applicable.	No Exceptions Noted
		Inspected the Access Control & Termination Policy, the listing of employees that were terminated within the review period, and the system user access listings and cross referenced them against the termination checklists for the total population of terminated personnel to determine that upon termination or when internal personnel no longer require access, system access was removed, as applicable.	No Exceptions Noted
	Users are provisioned access to systems based on principle of least privilege.	Inquired of management regarding user provisioning processes and access controls to determine that users were provisioned access to systems based on principle of least privilege.	No Exceptions Noted
		Inspected the Access Control & Termination Policy, the listing of employees that were onboarded within the review period, and access request	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Logical and Physical Access			
CC6.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		tickets for the total population of new hire employees & a sample of new contractors to determine that users are provisioned access to systems based on principle of least privilege.	
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 Access Control and Termination Policy governs authentication and access to applicable systems, data, and networks.	Inspected the Access Control & Termination Policy to determine that an Access Control and Termination Policy governed authentication and access to applicable systems, data, and networks.	No Exceptions Noted
	System owners conduct scheduled user access reviews of production servers, databases, and applications to validate internal user access is commensurate with job responsibilities.	Inquired of management regarding the user access review process to determine that system owners conducted scheduled user access reviews of production servers, databases, and applications to validate internal user access was commensurate with job responsibilities.	No Exceptions Noted
		Inspected the Access Control & Termination Policy and a sample bi-annual user access review report to determine that system owners conducted scheduled user access reviews of production servers, databases, and applications to validate	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Logical and Physical Access			
CC6.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		internal user access was commensurate with job responsibilities.	
	Upon termination or when internal personnel no longer require access, system access is removed, as applicable.	Inquired of management regarding the access removal and termination process to determine that upon termination or when internal personnel no longer required access, system access was removed, as applicable.	No Exceptions Noted
		Inspected the Access Control & Termination Policy, the listing of employees that were terminated within the review period, and the system user access listings and cross referenced them against the termination checklists for the total population of terminated personnel to determine that upon termination or when internal personnel no longer require access, system access was removed, as applicable.	No Exceptions Noted
	Users are provisioned access to systems based on principle of least privilege.	Inquired of management regarding user provisioning processes and access controls to determine that users were provisioned access to systems based on principle of least privilege.	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Logical and Physical Access			
CC6.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Inspected the Access Control & Termination Policy, the listing of employees that were onboarded within the review period, and access request tickets for the total population of new hire employees & a sample of new contractors to determine that users are provisioned access to systems based on principle of least privilege.	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.	**Subservice Organization:** This Criterion is the responsibility of a subservice organization provider. Reference Section III.		**N/A**
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from	A Data Retention and Disposal Policy specifies how customer data is to be retained and disposed of based on compliance requirements and contractual obligations.	Inquired of management regarding data retention and disposal practices to determine that a Data Retention and Disposal Policy specified how customer data was to be retained and disposed of based on compliance requirements and contractual obligations.	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Logical and Physical Access			
CC6.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
those assets has been diminished and is no longer required to meet the entity's objectives.		Inspected the Data Retention & Disposal Policy and the listing of data disposals due to retention guidelines within the review period to determine that a Data Retention and Disposal Policy specified how customer data was to be retained and disposed of based on compliance requirements and contractual obligations.	No Exceptions Noted
		Disclosure Noted: Tests of the control activity disclosed that no data disposals due to retention guidelines occurred within the review period, hence the operating effectiveness of the control cannot be determined.	Disclosure Noted
	Vendor SOC 2 reports (or equivalent) are collected and reviewed on at least an annual basis.	Inspected the Vendor Management Policy and the attestation reports & vendor reviews for a sample of vendors to determine that vendor SOC 2 reports (or equivalent) were collected and reviewed on at least an annual basis.	No Exceptions Noted
CC6.6 - The entity implements logical access security	A Network Security Policy identifies the requirements for protecting information and systems within and across networks.	Inspected the Network Security Policy to determine that a Network Security Policy identified the requirements for	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Logical and Physical Access			
CC6.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
measures to protect against threats from sources outside its system boundaries.		protecting information and systems within and across networks.	
	An Encryption and Key Management Policy supports the secure encryption and decryption of app secrets, and governs the use of cryptographic controls.	Inspected the Encryption and Key Management Policy to determine that an Encryption and Key Management Policy supported the secure encryption and decryption of app secrets, and governs the use of cryptographic controls.	No Exceptions Noted
	Configurations ensure available networking ports, protocols, services, and environments are restricted as necessary, including firewalls.	Inquired of management regarding firewall configurations and network security measures to determine that configurations ensured available networking ports, protocols, services, and environments were restricted as necessary, including firewalls.	No Exceptions Noted
		Observed the firewall and network configurations to determine that configurations ensured available networking ports, protocols, services, and environments were restricted as necessary, including firewalls.	No Exceptions Noted
		Inspected the Network Security Policy and the firewall configurations to determine that configurations ensured available networking ports, protocols,	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Logical and Physical Access			
CC6.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		services, and environments were restricted as necessary, including firewalls.	
	Personnel are required to use strong, complex passwords and a second form of authentication to access sensitive systems, networks, and information.	Inspected the Access Control & Termination Policy and the password & multi-factor authentication (MFA) configurations for the application, codebase, database, network, & operating system to determine that personnel were required to use strong, complex passwords and a second form of authentication to access sensitive systems, networks, and information.	No Exceptions Noted
	Security tools are implemented to provide monitoring of network traffic to the production environment.	Inspected the Network Security Policy, the alerting dashboard, the alert recipient listing, and a sample of alerts to determine to determine that security tools were implemented to provide monitoring of network traffic to the production environment.	No Exceptions Noted
	Service data transmitted over the internet is encrypted-in-transit.	Inspected the Encryption & Key Management Policy, the SSL configurations, and TLS configurations to determine that service data transmitted over the internet was encrypted-in-transit.	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Logical and Physical Access			
CC6.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	An Acceptable Use Policy defines standards for appropriate and secure use of company hardware and electronic systems including storage media, communication tools and internet access.	Inspected the Acceptable Use Policy to determine that an Acceptable Use Policy defined standards for appropriate and secure use of company hardware and electronic systems including storage media, communication tools and internet access.	No Exceptions Noted
	Company endpoints are managed and configured with anti-virus and hard drive encryption.	Inquired of management regarding endpoint security configurations to determine that Company endpoints were managed and configured with anti-virus and hard drive encryption.	No Exceptions Noted
		Inspected the Configuration & Asset Management Policy and the centralized encryption & anti-virus configurations for company owned workstations to determine that company endpoints were managed and configured with anti-virus and hard drive encryption.	No Exceptions Noted
	Service data is encrypted-at-rest.	Inspected the Encryption & Key Management Policy and the database encryption configurations to determine that service data was encrypted-at-rest.	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Logical and Physical Access			
CC6.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Service data transmitted over the internet is encrypted-in-transit.	Inspected the Encryption & Key Management Policy, the SSL configurations, and TLS configurations to determine that service data transmitted over the internet was encrypted-in-transit.	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.	A Change Management Policy governs the documenting, tracking, testing, and approving of system, network, security, and infrastructure changes.	Inspected the Change Management Policy to determine that a Change Management Policy governed the documenting, tracking, testing, and approving of system, network, security, and infrastructure changes.	No Exceptions Noted
	A Configuration and Asset Management Policy governs configurations for new sensitive systems.	Inspected the Configuration and Asset Management Policy to determine that a Configuration and Asset Management Policy governed configurations for new sensitive systems.	No Exceptions Noted
	An Acceptable Use Policy defines standards for appropriate and secure use of company hardware and electronic systems including storage media, communication tools and internet access.	Inspected the Acceptable Use Policy to determine that an Acceptable Use Policy defined standards for appropriate and secure use of company hardware and electronic systems including storage media, communication tools and internet access.	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Logical and Physical Access			
CC6.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Baseline configurations and codebases for production infrastructure, systems, and applications are securely managed.	Inquired of management regarding baseline configuration and codebase management practices to determine that baseline configurations and codebases for production infrastructure, systems, and applications were securely managed.	No Exceptions Noted
		Inspected the baseline codebase and infrastructure hardening configurations to determine that baseline configurations and codebases for production infrastructure, systems, and applications were securely managed.	No Exceptions Noted
	Company endpoints are managed and configured with anti-virus and hard drive encryption.	Inquired of management regarding endpoint security configurations to determine that Company endpoints were managed and configured with anti-virus and hard drive encryption.	No Exceptions Noted
		Inspected the Configuration & Asset Management Policy and the centralized encryption & anti-virus configurations for company owned workstations to determine that company endpoints were managed and configured with anti-virus and hard drive encryption.	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Logical and Physical Access			
CC6.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Software changes are tested prior to being deployed into production.	Inspected the Change Management Policy, the Secure Development Policy, the listing of code changes that occurred within the review period, and tickets for a sample of changes to determine that software changes were tested prior to being deployed into production.	No Exceptions Noted
	System changes are approved by at least 1 independent person prior to deployment into production.	Inspected the Change Management Policy, the Secure Development Policy, the listing of code changes that occurred within the review period, and tickets for a sample of changes to determine that system changes were approved by at least 1 independent person prior to deployment into production.	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
System Operations			
CC7.0	**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.	A Configuration and Asset Management Policy governs configurations for new sensitive systems.	Inspected the Configuration and Asset Management Policy to determine that a Configuration and Asset Management Policy governed configurations for new sensitive systems.	No Exceptions Noted
	A Vulnerability Management and Patch Management Policy outlines the processes to efficiently respond to identified vulnerabilities.	Inspected the Vulnerability Management and Patch Management Policy to determine that a Vulnerability Management and Patch Management Policy outlined the processes to efficiently respond to identified vulnerabilities.	No Exceptions Noted
	A third party is engaged to conduct a network and application penetration test of the production environment at least annually. Critical and high-risk findings are tracked through resolution.	Inquired of management regarding penetration testing practices and remediation processes to determine that a third party was engaged to conduct a network and application penetration test of the production environment at least annually and that critical and high-risk findings were tracked through resolution.	No Exceptions Noted
		Inspected the Vulnerability Management Policy, penetration test statement of work, and penetration test scoping documentation to determine that a third party was engaged to conduct a network and	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
System Operations			
CC7.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		application penetration test of the production environment at least annually and critical and high-risk findings were tracked through resolution.	
	Alerting software is used to notify impacted teams of potential security events.	Inspected the Network Security Policy, the alerting dashboard, the alert recipient listing, and a sample of alerts to determine that alerting software was used to notify impacted teams of potential security events.	No Exceptions Noted
	Baseline configurations and codebases for production infrastructure, systems, and applications are securely managed.	Inquired of management regarding baseline configuration and codebase management practices to determine that baseline configurations and codebases for production infrastructure, systems, and applications were securely managed.	No Exceptions Noted
		Inspected the baseline codebase and infrastructure hardening configurations to determine that baseline configurations and codebases for production infrastructure, systems, and applications were securely managed.	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
System Operations			
CC7.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Logging and monitoring software is used to collect data from infrastructure to detect potential security threats, unusual system activity, and monitor system performance, as applicable.	Inspected the Network Security Policy, the logging dashboard, the listing of alert recipients, and a sample of alerts that were sent within the review period to determine that logging and monitoring software was used to collect data from infrastructure to detect potential security threats, unusual system activity, and monitor system performance, as applicable.	No Exceptions Noted
	Security tools are implemented to provide monitoring of network traffic to the production environment.	Inspected the Network Security Policy, the alerting dashboard, the alert recipient listing, and a sample of alerts to determine to determine that security tools were implemented to provide monitoring of network traffic to the production environment.	No Exceptions Noted
	Vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis.	Inquired of management regarding vulnerability scanning practices and remediation processes to determine that vulnerability scanning was performed on production infrastructure systems, and identified deficiencies were remediated on a timely basis.	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
System Operations			
CC7.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Inspected the Vulnerability & Patch Management Policy, the listing of vulnerabilities identified during host based & dependency scans, and remediation tickets for a sample of vulnerabilities identified during dependency scanning to determine that vulnerability scanning was performed on production infrastructure systems, and identified deficiencies were remediated on a timely basis.	No Exceptions Noted
		Disclosure Noted: Tests of the control activity disclosed that no critical or high vulnerabilities were identified during host-based vulnerability scans within the review period, hence the operating effectiveness of the control cannot be determined.	Disclosure Noted
CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters,	A Network Security Policy identifies the requirements for protecting information and systems within and across networks.	Inspected the Network Security Policy to determine that a Network Security Policy identified the requirements for protecting information and systems within and across networks.	No Exceptions Noted
	Alerting software is used to notify impacted teams of potential security events.	Inspected the Network Security Policy, the alerting dashboard, the alert recipient listing, and a sample of alerts	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
System Operations			
CC7.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.		to determine that alerting software was used to notify impacted teams of potential security events.	
	Logging and monitoring software is used to collect data from infrastructure to detect potential security threats, unusual system activity, and monitor system performance, as applicable.	Inspected the Network Security Policy, the logging dashboard, the listing of alert recipients, and a sample of alerts that were sent within the review period to determine that logging and monitoring software was used to collect data from infrastructure to detect potential security threats, unusual system activity, and monitor system performance, as applicable.	No Exceptions Noted
	Security tools are implemented to provide monitoring of network traffic to the production environment.	Inspected the Network Security Policy, the alerting dashboard, the alert recipient listing, and a sample of alerts to determine to determine that security tools were implemented to provide monitoring of network traffic to the production environment.	No Exceptions Noted
CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a	An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution.	Inspected the Security Incident Response Plan to determine that the company had an Incident Response Plan that outlined the process of identifying, prioritizing, communicating,	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
System Operations			
CC7.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.		assigning and tracking confirmed incidents through to resolution.	
	Identified incidents are documented, tracked, and analyzed according to the Incident Response Plan.	Inquired of management regarding incident documentation and tracking processes to determine that identified incidents were documented, tracked, and analyzed according to the Incident Response Plan.	No Exceptions Noted
		Inspected the Security Incident Response Plan and the listing of incidents that occurred within the review period to determine that identified incidents were documented, tracked, and analyzed according to the Incident Response Plan.	No Exceptions Noted
		Disclosure Noted: Tests of the control activity disclosed that no incidents occurred within the review period, hence the operating effectiveness of the control cannot be determined.	Disclosure Noted
CC7.4 - The entity responds to identified security incidents by executing a defined incident response program to understand,	After any identified security incident has been resolved, management provides a "Lessons Learned" document to the team in order to continually improve security and operations.	Inquired of management regarding the security incident resolution process to determine that after any identified security incident had been resolved, management provided a "Lessons Learned" document to the team in	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
System Operations			
CC7.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
contain, remediate, and communicate security incidents, as appropriate.		order to continually improve security and operations.	
		Inspected the Security Incident Response Plan and the listing of incidents that occurred within the review period to determine that after any identified security incident had been resolved, management provided a "Lessons Learned" document to the team in order to continually improve security and operations.	No Exceptions Noted
		Disclosure Noted: Tests of the control activity disclosed that no incidents occurred within the review period, hence the operating effectiveness of the control cannot be determined.	Disclosure Noted
	An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution.	Inspected the Security Incident Response Plan to determine that the company had an Incident Response Plan that outlined the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution.	No Exceptions Noted
	Business Continuity and Disaster Recovery Policy governs required processes for restoring the service	Inspected the Business Continuity and Disaster Recovery Policy to determine that business Continuity and Disaster	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
System Operations			
CC7.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	or supporting infrastructure after suffering a disaster or disruption.	Recovery Policy governed required processes for restoring the service or supporting infrastructure after suffering a disaster or disruption.	
	Critical information is communicated to external parties, as applicable.	Inspected the Terms of Service, the application status page, and a sample of change notifications to determine that critical information was communicated to external parties, as applicable.	No Exceptions Noted
	Identified incidents are documented, tracked, and analyzed according to the Incident Response Plan.	Inquired of management regarding incident documentation and tracking processes to determine that identified incidents were documented, tracked, and analyzed according to the Incident Response Plan.	No Exceptions Noted
		Inspected the Security Incident Response Plan and the listing of incidents that occurred within the review period to determine that identified incidents were documented, tracked, and analyzed according to the Incident Response Plan.	No Exceptions Noted
		Disclosure Noted: Tests of the control activity disclosed that no incidents occurred within the review period,	Disclosure Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
System Operations			
CC7.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		hence the operating effectiveness of the control cannot be determined.	
	Personnel who violate information security policies are subject to disciplinary action and such disciplinary action is clearly documented in one or more policies.	Inquired of management regarding disciplinary action processes for information security policy violations to determine that personnel who violated information security policies were subject to disciplinary action and such disciplinary action was clearly documented in one or more policies.	No Exceptions Noted
		Inspected the Code of Conduct to determine that personnel who violated information security policies were subject to disciplinary action and such disciplinary action was clearly documented in one or more policies.	No Exceptions Noted
		Disclosure Noted: Tests of the control activity disclosed that no disciplinary actions were taken within the review period, hence the operating effectiveness of the control cannot be determined.	Disclosure Noted
	The Incident Response Plan is periodically tested via tabletop exercises or equivalents. When necessary,	Inquired of management regarding incident response testing practices to determine that the Incident Response Plan was periodically tested via	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
System Operations			
CC7.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Management makes changes to the Incident Response Plan based on the test results.	tabletop exercises or equivalents and that, when necessary, management made changes to the Incident Response Plan based on the test results.	
		Inspected the Security Incident Response Plan and the annual incident response tabletop exercise to determine that the Incident Response Plan was periodically tested via tabletop exercises or equivalents and that, when necessary, management made changes to the Incident Response Plan based on the test results.	No Exceptions Noted
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.	After any identified security incident has been resolved, management provides a "Lessons Learned" document to the team in order to continually improve security and operations.	Inquired of management regarding the security incident resolution process to determine that after any identified security incident had been resolved, management provided a "Lessons Learned" document to the team in order to continually improve security and operations.	No Exceptions Noted
		Inspected the Security Incident Response Plan and the listing of incidents that occurred within the review period to determine that after	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
System Operations			
CC7.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		any identified security incident had been resolved, management provided a "Lessons Learned" document to the team in order to continually improve security and operations.	
		Disclosure Noted: Tests of the control activity disclosed that no incidents occurred within the review period, hence the operating effectiveness of the control cannot be determined.	Disclosure Noted
	An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution.	Inspected the Security Incident Response Plan to determine that the company had an Incident Response Plan that outlined the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution.	No Exceptions Noted
	Backed-up data is restored to a non-production environment at least annually to validate the integrity of backups.	Inquired of management regarding backup restoration and testing practices to determine that backed-up data was restored to a non-production environment at least annually to validate the integrity of backups.	No Exceptions Noted
		Inspected the Business Continuity & Disaster Recovery Plan to determine that backed-up data was restored to a	Exception noted. Reference Section

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
System Operations			
CC7.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		non-production environment at least annually to validate the integrity of backups.	V for further detail.
	Critical information is communicated to external parties, as applicable.	Inspected the Terms of Service, the application status page, and a sample of change notifications to determine that critical information was communicated to external parties, as applicable.	No Exceptions Noted
	Identified incidents are documented, tracked, and analyzed according to the Incident Response Plan.	Inquired of management regarding incident documentation and tracking processes to determine that identified incidents were documented, tracked, and analyzed according to the Incident Response Plan.	No Exceptions Noted
		Inspected the Security Incident Response Plan and the listing of incidents that occurred within the review period to determine that identified incidents were documented, tracked, and analyzed according to the Incident Response Plan.	No Exceptions Noted
		Disclosure Noted: Tests of the control activity disclosed that no incidents occurred within the review period,	Disclosure Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
System Operations			
CC7.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		hence the operating effectiveness of the control cannot be determined.	
	The Business Continuity and Disaster Recovery Plan is periodically tested via tabletop exercises or equivalents. When necessary, Management makes changes to the Business Continuity and Disaster Recovery Plan based on the test results.	Inspected the Business Continuity & Disaster Recovery Plan and the annual tabletop exercise to determine that the Business Continuity and Disaster Recovery Plan was periodically tested via tabletop exercises or equivalents and when necessary, Management made changes to the Business Continuity and Disaster Recovery Plan based on the test results.	No Exceptions Noted
	The Incident Response Plan is periodically tested via tabletop exercises or equivalents. When necessary, Management makes changes to the Incident Response Plan based on the test results.	Inquired of management regarding incident response testing practices to determine that the Incident Response Plan was periodically tested via tabletop exercises or equivalents and that, when necessary, management made changes to the Incident Response Plan based on the test results.	No Exceptions Noted
		Inspected the Security Incident Response Plan and the annual incident response tabletop exercise to determine that the Incident Response Plan was periodically tested via tabletop exercises or equivalents and	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
System Operations			
CC7.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		that, when necessary, management made changes to the Incident Response Plan based on the test results.	

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Change Management			
CC8.0	**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.	A Change Management Policy governs the documenting, tracking, testing, and approving of system, network, security, and infrastructure changes.	Inspected the Change Management Policy to determine that a Change Management Policy governed the documenting, tracking, testing, and approving of system, network, security, and infrastructure changes.	No Exceptions Noted
	A Configuration and Asset Management Policy governs configurations for new sensitive systems.	Inspected the Configuration and Asset Management Policy to determine that a Configuration and Asset Management Policy governed configurations for new sensitive systems.	No Exceptions Noted
	A Secure Development Policy defines the requirements for secure software and system development and maintenance.	Inspected the Secure Development Policy to determine that a Secure Development Policy defined the requirements for secure software and system development and maintenance.	No Exceptions Noted
	Baseline configurations and codebases for production infrastructure, systems, and applications are securely managed.	Inquired of management regarding baseline configuration and codebase management practices to determine that baseline configurations and codebases for production infrastructure, systems, and applications were securely managed.	No Exceptions Noted
		Inspected the baseline codebase and infrastructure hardening configurations to determine that baseline	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Change Management			
CC8.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		configurations and codebases for production infrastructure, systems, and applications were securely managed.	
	Development, staging, and production environments are segregated.	Inspected the segmented production & development environments to determine that development, staging, and production environments were segregated.	No Exceptions Noted
	Production data is not used in the development and testing environments, unless required for debugging customer issues.	Inquired of management regarding data usage practices across environments to determine that production data was not used in the development and testing environments, unless required for debugging customer issues.	No Exceptions Noted
		Observed the development and testing environment configurations and data sources to determine that production data was not used in the development and testing environments, unless required for debugging customer issues.	No Exceptions Noted
		Inspected the segregated development and production environments to determine that production data was not used in the development and	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Change Management			
CC8.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		testing environments, unless required for debugging customer issues.	
	Software changes are tested prior to being deployed into production.	Inspected the Change Management Policy, the Secure Development Policy, the listing of code changes that occurred within the review period, and tickets for a sample of changes to determine that software changes were tested prior to being deployed into production.	No Exceptions Noted
	System changes are approved by at least 1 independent person prior to deployment into production.	Inspected the Change Management Policy, the Secure Development Policy, the listing of code changes that occurred within the review period, and tickets for a sample of changes to determine that system changes were approved by at least 1 independent person prior to deployment into production.	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Risk Mitigation			
CC9.0	**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.	A Risk Assessment and Treatment Policy governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners. Risk tolerance and strategies are also defined in the policy.	Inspected the Risk Assessment and Treatment Policy to determine that a Risk Assessment and Treatment Policy governed the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners, and that risk tolerance and strategies were also defined in the policy.	No Exceptions Noted
	A risk register is maintained, which records the risk mitigation strategies for identified risks, and the development or modification of controls consistent with the risk mitigation strategy.	Inspected the Risk Assessment & Treatment Policy and the annual risk assessment report to determine that a risk register was maintained, which recorded the risk mitigation strategies for identified risks, and the development or modification of controls consistent with the risk mitigation strategy.	No Exceptions Noted
	An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution.	Inspected the Security Incident Response Plan to determine that the company had an Incident Response Plan that outlined the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution.	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Risk Mitigation			
CC9.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Business Continuity and Disaster Recovery Policy governs required processes for restoring the service or supporting infrastructure after suffering a disaster or disruption.	Inspected the Business Continuity and Disaster Recovery Policy to determine that business Continuity and Disaster Recovery Policy governed required processes for restoring the service or supporting infrastructure after suffering a disaster or disruption.	No Exceptions Noted
	Cybersecurity insurance has been procured to help minimize the financial impact of cybersecurity loss events.	Inspected the cybersecurity insurance policies with coverage of the entire review period to determine that cybersecurity insurance had been procured to help minimize the financial impact of cybersecurity loss events.	No Exceptions Noted
	Formal risk assessments are performed, which includes the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Inspected the Risk Assessment & Treatment Policy and the annual risk assessment report to determine that formal risk assessments were performed, which included the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	No Exceptions Noted
CC9.2 - The entity assesses and manages risks associated with	A Vendor Risk Management Policy defines a framework for the onboarding and management of the vendor relationship lifecycle.	Inspected the Vendor Management Policy to determine that a Vendor Risk Management Policy defined a framework for the onboarding and	No Exceptions Noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
Risk Mitigation			
CC9.0	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
vendors and business partners.		management of the vendor relationship lifecycle.	
	Vendor SOC 2 reports (or equivalent) are collected and reviewed on at least an annual basis.	Inspected the Vendor Management Policy and the attestation reports & vendor reviews for a sample of vendors to determine that vendor SOC 2 reports (or equivalent) were collected and reviewed on at least an annual basis.	No Exceptions Noted

SECTION 5

OTHER INFORMATION PROVIDED BY MANAGEMENT

MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS				
Control Criteria	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**	**Management's Response**
CC7.5	Backed-up data is restored to a non-production environment at least annually to validate the integrity of backups.	Inspected the Business Continuity & Disaster Recovery Plan to determine that backed-up data was restored to a non-production environment at least annually to validate the integrity of backups.	Sentry Assurance noted that Aline Technologies did not conduct a backup restoration test on production data within the review period as apart of business continuity and disaster recovery operations.	During the review period, Aline Technologies maintained automated backups for all production data, including AWS RDS, ElastiCache, and other critical infrastructure components. A backup restoration test was performed during the review period to validate the integrity of backups; however, evidence of the restoration (e.g., screenshots and formal documentation) was not retained in accordance with the control's documentation requirements. Upon identification of this exception, management reinforced documentation procedures to ensure that all future backup restoration tests are formally documented and retained. A standardized evidence retention process has been implemented to

MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS				
Control Criteria	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**	**Management's Response**
				capture restoration logs, screenshots, and supporting artifacts. Management will continue to perform and formally document backup restoration testing at least annually in accordance with the Business Continuity & Disaster Recovery Plan.
CC5.3	Internal personnel review and accept applicable information security policies at least annually.	Inspected the suite of information security policies, the listing of current internal personnel, and policy acknowledgments for a sample of internal personnel to determine that internal personnel review and accept applicable information security policies at least annually.	Sentry Assurance noted that Aline Technologies did not capture acknowledgements of information security policies for the total population of five new hires onboarded within the review period.	During the review period, Aline Technologies maintained information security policies requiring annual review and acknowledgment by internal personnel. Due to a misconfiguration in the Secureframe compliance management system, acknowledgments for five new hires were not issued or captured timely. Upon discovery, the misconfiguration was corrected, and the affected personnel completed policy review and acknowledgment immediately. Management

MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS				
Control Criteria	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**	**Management's Response**
				has reviewed and validated Secureframe configuration settings and implemented periodic administrative reviews to ensure onboarding workflows properly trigger policy acknowledgment requirements for all new hires. Management will continue to monitor compliance with policy acknowledgment requirements on an ongoing basis.
CC1.4, CC2.2	Internal personnel complete annual training programs for information security to help them understand their obligations and responsibilities related to security.	Inspected the Information Security Policy, the listing of current employees & employees that were onboarded within the review period, and information security awareness training records for a sample of current employees & the total population of new hires to determine that internal personnel completed annual training programs for information security to help them understand their obligations and responsibilities related to security.	Sentry Assurance noted that Aline Technologies did not issue or capture completion of security awareness training for the total population of five new hires onboarded within the review period.	During the review period, Aline Technologies required all internal personnel to complete annual security awareness training. Due to the same Secureframe configuration issue affecting policy acknowledgments, security awareness training was not issued or tracked for five new hires within the required timeframe. Once identified, the configuration issue was

MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS				
Control Criteria	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**	**Management's Response**
				remediated, and the affected personnel completed security awareness training promptly. Management has implemented additional onboarding verification procedures to ensure that all new hires are enrolled in and complete required security awareness training in a timely manner. Ongoing monitoring controls have been established to prevent recurrence.