System and Organization Controls Report (SOC 2® Type 2)

Report on Deal Engine, Inc.'s Description of Its Automated Refunds and Changes Platform and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security Throughout the Period September 1, 2024, to September 30, 2025

Deal Engine

INSIGHT ASSURANCE

☎ +1 877.607.7727

www.InsightAssurance.com

TABLE OF CONTENTS

SECTION 1:
INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Deal Engine, Inc.

Scope

We have examined Deal Engine, Inc.'s ("Deal Engine" or "the service organization") accompanying description of its Automated Refunds and Changes Platform found in Section 3 titled "Deal Engine, Inc.'s description of its Automated Refunds and Changes Platform" throughout the period September 1, 2024, to September 30, 2025, ("description") based on the criteria for a description of a service organization's system set forth in DC section 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 September 1, 2024, to September 30, 2025, to provide reasonable assurance that Deal Engine's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA*, Trust Services Criteria.*

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

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Deal Engine, to achieve Deal Engine's service commitments and system requirements based on the applicable trust services criteria. The description presents Deal Engine's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Deal Engine's controls. Our examination did not include such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such controls.

The information included in Section 5, “Other Information Provided by Deal Engine, Inc.,” is presented by Deal Engine management to provide additional information and is not part of the description. Information about Deal Engine management’s responses to exceptions has not been subjected to the procedures applied in the examination of the description and the suitability of the design and operating effectiveness of controls to achieve Deal Engine’s service commitments and system requirements based on the applicable trust services criteria, and accordingly, we express no opinion on it.

Service Organization’s Responsibilities

Deal Engine is responsible for its service commitments and system requirements and designing, implementing, and operating effective controls within the system to provide reasonable assurance that Deal Engine’s service commitments and system requirements were achieved. In Section 2, Deal Engine has provided the accompanying assertion titled “Deal Engine, Inc.’s Management Assertion” (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. Deal Engine is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria, and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization’s service commitments and system requirements.

Service Auditor’s Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and meet our other ethical responsibilities in accordance with ethical requirements relating to the examination engagement.

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 or did not operate effectively.
- performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.

- performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

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. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Test of Controls

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

Opinion

In our opinion, in all material respects,

- the description presents Deal Engine's Automated Refunds and Changes Platform that was designed and implemented throughout the period September 1, 2024, to September 30, 2025, in accordance with the description criteria.
- the controls stated in the description were suitably designed throughout the period September 1, 2024, to September 30, 2025, to provide reasonable assurance that Deal Engine'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 organizations and user entities applied the complementary controls assumed in the design of Deal Engine's controls throughout that period.
- the controls stated in the description operated effectively throughout the period September 1, 2024, to September 30, 2025, to provide reasonable assurance that Deal Engine's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and

user entity controls assumed in the design of Deal Engine's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of management of Deal Engine; user entities of Deal Engine's Automated Refunds and Changes Platform during some or all of the period September 1, 2024, to September 30, 2025; business partners of Deal Engine subject to risks arising from interactions with the Automated Refunds and Changes Platform; 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 user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

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

Insight Compliance LLC

dba Insight Assurance
Tampa, Florida
January 30, 2026

SECTION 2:
DEAL ENGINE, INC.'S MANAGEMENT ASSERTION

DEAL ENGINE, INC.’S MANAGEMENT ASSERTION

We have prepared the description of Deal Engine, Inc.’s (“Deal Engine” or “the service organization”) Automated Refunds and Changes Platform entitled “Deal Engine, Inc.’s description of its Automated Refunds and Changes Platform” throughout the period September 1, 2024, to September 30, 2025, (“description”) based on the criteria for a description of a service organization’s system set forth in DC section 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 Automated Refunds and Changes Platform that may be useful when assessing the risks arising from interactions with Deal Engine’s system, particularly information about system controls that Deal Engine has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA*, Trust Services Criteria.*

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

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

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

- the description presents Deal Engine’s Automated Refunds and Changes Platform that was designed and implemented throughout the period September 1, 2024, to September 30, 2025, in accordance with the description criteria.
- the controls stated in the description were suitably designed throughout the period September 1, 2024, to September 30, 2025, to provide reasonable assurance that Deal Engine’s service commitments and system requirements would be achieved based on the applicable trust services criteria, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Deal Engine’s controls.
- the controls stated in the description operated effectively throughout the period September 1, 2024, to September 30, 2025, to provide reasonable assurance that Deal

Engine's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of Deal Engine's controls operated effectively throughout that period.

Deal Engine, Inc.
January 30, 2026

SECTION 3: DEAL ENGINE, INC.'S DESCRIPTION OF ITS AUTOMATED REFUNDS AND CHANGES PLATFORM

DEAL ENGINE, INC.'S DESCRIPTION OF ITS AUTOMATED REFUNDS AND CHANGES PLATFORM

COMPANY BACKGROUND

Deal Engine was founded in March 2017 by Alexandro Jara to provide Software as a service in the airline refund industry. The organization is based out of Miami, Florida, with additional sites in Mexico City.

DESCRIPTION OF SERVICES OVERVIEW

Automated Refunds and Changes Platform is an online platform [or Application Programming Interface (API)] that enables automatic quoting, processing, and tracking of large quantities of refunds from one place in real time. The platform provides reporting via API and digital dashboards. The platform receives all refund requests in two ways: via the API or the user interface. The Artificial Intelligence (A.I.) algorithms calculate the exact refund amount, reading and interpreting the ticket's fare and tax rules. Refund requests are validated by an agent or traveler before being automatically processed through Billing and Settlement Plan (BSP), Airlines Reporting Corporation (ARC), or Global Distribution System (GDS). Refund requests are processed and reflected on the client user interface.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Deal Engine designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Deal Engine makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that the Company has established for the services. The system services are subject to the Security commitments established internally for its services. Deal Engine designs its processes and procedures related to the system to meet its objectives.

Commitments to customers are documented and communicated in customer agreements, as well as in the description of the service offered provided online.

Security Commitments

Security commitments include, but are not limited to, the following:

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role.
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system.
- Regular vulnerability scans over the system and network, and penetration tests over the production environment.
- Operational procedures for managing security incidents and breaches, including notification procedures.
- Use of encryption technologies to protect customer data both at rest and in transit.
- Use of data retention and data disposal.

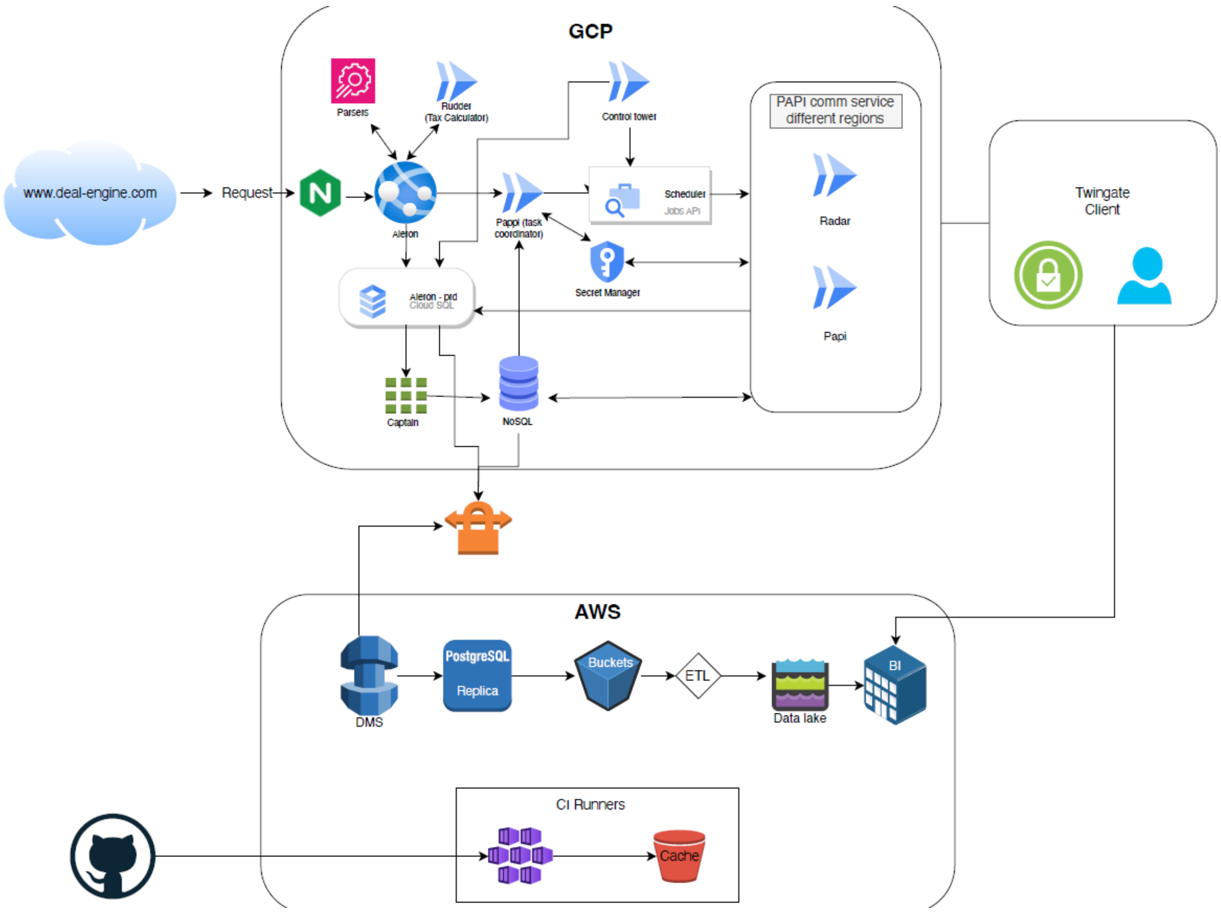
COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

The System description is comprised of the following components:

- **Infrastructure –** The collection of physical or virtual resources that supports an overall Information Technology (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 support 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 are mobile applications or desktop or laptop applications.
- **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

Deal Engine maintains a system inventory that includes virtual machines, computers (desktops and laptops), and networking devices (switches and routers). The inventory documents device name, inventory type, description, and owner. To outline the topology of its network, the organization maintains the following network diagram.



The in-scope infrastructure components are shown in the table below:

Primary Infrastructure		
Asset	**Type**	**Purpose**
AWS Elastic Compute Cloud (EC2)	AWS	Virtual machines that are used as servers to run the Elastic Kubernetes Service (EKS) Cluster or other services like reverse proxies, load balancers, containerized application deployments, etc.
AWS Elastic Load Balancers	AWS	Load balance internal and external traffic
Virtual Private Cloud (VPC)	AWS	Protects the network perimeter and restricts inbound and outbound access
S3 Buckets	AWS	Storage, upload and download
Amazon Relational Database Service (RDS)	AWS	Database
AWS ElastiCache for Redis	AWS	In-memory Database
AWS EKS	AWS	Managed Kubernetes cluster that runs the applications and services

Primary Infrastructure		
Asset	**Type**	**Purpose**
Google Cloud Load Balancing (GLB)	GCP	Load balance internal and external traffic
Google Kubernetes Engine (GKE)	GCP	Runs container workloads
Google Cloud Storage	GCP	Data storage
Google Cloud Functions	GCP	Serverless function execution
Google Cloud Tasks	GCP	Asynchronous task execution
Google Cloud VPC	GCP	Protects the network perimeter and restricts inbound and outbound access
Google Cloud Logging	GCP	Operational logs
Google Cloud Run	GCP	Managed server execution
Google Cloud SQL DB	GCP	Data storage

SOFTWARE

Deal Engine is responsible for managing the development and operation of the system. The software supporting the system consists of the applications, programs, and other software components used to build, secure, maintain, and monitor the system. The list of software is shown in the table below.

Primary Software	
System/Application	**Purpose**
GitHub	Code management tool
Google Workspace	Workspaces

PEOPLE

The company employs dedicated team members to handle major product functions, including operations and support. The IT/Engineering Team monitors the environment, as well as manages data backups and recovery. The Company focuses on hiring the right people for the right job, as well as training them both in their specific tasks and on the ways to keep the company and its data secure.

Deal Engine has a staff of approximately 56 organized in the following functional areas:

Chief Executive Officer (CEO) – Highest ranking executive, responsible for the overall strategy of the company, leading the company, and acting as the figurative head of the organization when communicating with stockholders, government entities, and the general public.

Chief Technology Officer (CTO) – Executive responsible for the company’s technological needs and oversees the effectiveness of the company’s technology resources.

Head of Product and Security – Responsible for overseeing product development, security strategy, and ensuring Deal Engine complies with all security related topics.

Chief Operating Officer (COO) – Responsible for designing and implementing processes and policies to ensure the continuous operation of the services and products, and overseas operations of the company.

Operations – Responsible for maintaining the availability of production infrastructure and managing access and Security for production infrastructure. Only members of the Operations team have access to the production environment. Members of the Operations team may also be members of the Engineering team.

DATA

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements. Customer data is captured, which is utilized by Deal Engine in delivering its Automated Refunds and Changes Platform services.

All employees and contractors of the company are obligated to respect and, in all cases, to protect customer data. Additionally, Deal Engine has policies and procedures in place for proper and secure handling of customer data. These policies and procedures are reviewed at least annually.

Data is classified into three major categories as outlined in the Data Management Policy:

Data		
Category	**Description**	**Examples**
Confidential	Highly sensitive data requires the highest levels of protection; access is restricted to specific employees or departments, and these records can only be passed to others with approval from the data owner, or a company executive.	• Customer Data • Personally identifiable information (PII) • Company financial and banking data • Salary, compensation and payroll information • Strategic plans • Incident reports • Risk assessment reports • Technical vulnerability reports

Data		
Category	**Description**	**Examples**
Restricted	Deal Engine proprietary information requiring thorough protection; access is restricted to employees with a “need-to-know” based on business requirements. This data can only be distributed outside the company with approval. This is default for all company information unless stated otherwise.	• Internal policies and internal legal documents • Meeting minutes and presentations • Contracts • Internal reports • Keybase messages • Email
Public	Documents intended for public consumption, which can be freely distributed outside Deal Engine.	• Marketing materials • Product descriptions • Release notes • External facing policies

PROCEDURES

Management has developed and communicated policies and procedures involved in the operation of the system. These procedures are developed in alignment with the overall Information Security Policy and are reviewed, updated, and approved as necessary for changes in the business at least annually. The following provides a summary of Deal Engine’s policies and procedures that comprise the internal control for the system.

Physical Security

Deal Engine’s production servers are maintained by AWS and GCP. Physical and environmental security protections are the responsibility of AWS and GCP. Deal Engine reviews the attestation reports and performs a risk analysis of AWS and GCP on at least an annual basis.

Logical Access

Deal Engine provides employees and contractors access to infrastructure via a role-based access control system, to ensure uniform, least privileged access to identified users and to maintain simple user provisioning and deprovisioning processes.

Access to these systems is split into admin roles, user roles, and no-access roles. User access and roles are reviewed on a quarterly basis to ensure the least privileged access.

The CTO is responsible for provisioning access to the system based on the employee’s role and performing a background check. The employee is responsible for reviewing Deal Engine’s policies and completing the security training.

When an employee is terminated, the CTO is responsible for deprovisioning access to all in-scope systems within 24 business hours of the employee’s termination.

Change Management

Deal Engine maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

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

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

Patch Management

Deal Engine takes a proactive approach to patch management. The Engineering Team regularly monitors through different tools where advanced notifications of bug-related patches are often disclosed prior to a public announcement by the vendor. This allows the company to plan for upcoming patches.

The Engineering Team reviews the availability of patches and independently determines if it is necessary to deploy them within the production environment. Approved patches are scheduled for installation in the test environment weekly, monthly or when it is required. If there are no issues in the test environment after a week, the patch will be applied to the production environment. The patching process is tracked via GitHub.

Backups and Recovery

Customer data is backed up and monitored by the CTO for completion and exceptions. If there is an exception, the CTO performs troubleshooting to identify the root cause and either reruns the backup or includes it as part of the next scheduled backup job.

Backup infrastructure is maintained by AWS and GCP, with physical access restricted according to the policies. Backups are encrypted, with access restricted to key personnel.

Computer Operations

Deal Engine maintains an Incident Response Plan to guide employees on reporting and responding to any information security events or incidents. Procedures are in place for identifying, reporting, and acting upon breaches or other incidents.

Deal Engine internally monitors all applications, including the web UI, databases, and cloud storage to ensure that service delivery matches Service Level Agreement (SLA) requirements.

Deal Engine utilizes vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open-source dependencies and maintains an internal SLA for responding to those issues.

Problem Management

Deal Engine maintains an Incident Response Plan that describes the process for identifying and addressing potential security incidents. The policy details exactly what must occur if an incident is suspected and covers both electronic and physical security incidents. Plans for detecting, responding to, and recovering from incidents are included in the policy, and post-incident activity requirements are defined. To ensure responsible employees are prepared to respond to incidents, the organization provides formal security breach training.

The organization provides a customer service request form where clients can report potential security breaches, and clients are also provided with an email and phone number for this same purpose. Internal users are directed to report incidents through an internal portal for documentation and tracking purposes.

Data Communications

Deal Engine has elected to use AWS and GCP to run its production infrastructure in part to avoid the complexity of network monitoring, configuration, and operations. AWS and GCP simplify the logical network configuration by providing an effective firewall around all the Deal Engine application containers, with the only ingress from the network via HTTPS connections to designated web frontend endpoints.

AWS and GCP also automate the provisioning and deprovisioning of containers to match the desired configuration; if an application container fails, it will be automatically replaced, regardless of whether that failure is in the application or on the underlying hardware.

Deal Engine engages an external security firm to perform annual penetration testing to identify potential vulnerabilities. In addition, automated vulnerability scans are conducted on a quarterly basis, and the product engineering team responds to any issues identified via the regular incident response and change management process.

System Monitoring

The Operations Security Policy describes the organization’s policies and procedures related to network logging and monitoring, as well as vulnerability identification and remediation. The organization uses CloudWatch and GCP Logs Explorer for system logging within the AWS and GCP environments, respectively.

The organization collects logs from the firewall and IDS. CloudWatch logs and firewall logs document source IP, destination IP, port, protocol type, and timestamp. The organization monitors system capacity using CloudWatch and GCP Logs Explorer.

The vulnerability assessment process involves the execution of Center for Internet Security (CIS) testing, implementation of antivirus software, and system patching. The organization uses a container to deploy the application and prohibit end-users from disabling or altering the software. This applies for both Cloud solutions.

Alerts are sent immediately when a potential virus is detected, and logs are generated and retained for at least one year, with at least three months readily available. Vulnerability scanning is used to identify newly emerging vulnerabilities, and the organization monitors vendors for patch updates to correct vulnerabilities.

Vendor Management

The organization maintains a Third-Party Management Policy that includes requirements for interacting with vendors/service providers. The policy includes requirements for performing due diligence measures prior to engaging with a new provider. Due diligence procedures include evaluating each material IT vendor's cost-effectiveness, functionality/services, risk, financial viability, compliance, and performance.

The organization is required to define service levels when negotiating an arrangement with a new vendor or re-negotiating an existing arrangement, and all service levels are agreed upon and documented clearly. The organization monitors its providers' service levels to ensure each provider is providing the agreed-upon services and is compliant with all requirements. The organization executes non-disclosure agreements with third parties before any information is shared.

Boundaries of the System

The boundaries of the Automated Refunds and Changes Platform are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the Automated Refunds and Changes Platform.

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

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

CONTROL ENVIRONMENT

The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across an organization. The organizational structure, separation of job responsibilities by departments and business function, documentation of policies and procedures, and internal audits are the methods used to define, implement, and assure effective operational controls. Senior management establish the tone at the top regarding the importance of internal control and expected standards of conduct.

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Deal

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

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

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

Management Philosophy and Operating Style

The Deal Engine management team must balance two competing interests: continuing to grow and develop in a cutting-edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly sensitive data and workflows customers entrust to Deal Engine.

The management team frequently meets to be briefed on technology changes that impact the way Deal Engine can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally, any regulatory changes that may require Deal Engine to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with Deal Engine’s core product offerings and duties to new and existing customers.

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

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

Commitment to Competence

Deal Engine's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees’ roles and responsibilities. Management’s commitment to competence includes management’s consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

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

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

Organizational Structure and Assignment of Authority and Responsibilities

Deal Engine's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

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

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

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

Human Resources Policies and Procedures

Deal Engine has formal hiring procedures that are designed to ensure that new team members are able to meet or exceed the job requirements and responsibilities. All candidates go through interviews and assessments of their education, professional experience, and certifications. Background checks are performed for all newly hired employees and include a review of their education and criminal records.

During the onboarding process, the new employees review the Code of Conduct and any other relevant policies and procedures relevant to their role. Newly hired employees are required to sign an acknowledgment of receipt and understanding of the Code of Conduct. These policies and procedures are also available to employees through the internal policies repository. Security awareness training is also completed at least annually by all employees, which includes the areas of security and confidentiality, to communicate the security implications around their roles and how their actions could affect the organization.

Ongoing performance feedback is provided to all employees. Formal performance reviews are completed annually by management to discuss expectations, goals, and the employees' performance for the last fiscal year.

RISK ASSESSMENT PROCESS

Deal Engine's risk assessment process identifies and manages risks that could potentially affect Deal Engine's ability to provide reliable and secure services to Deal Engine's customers. As part of this process, Deal Engine maintains a risk register to track all systems and procedures that could present risks to meeting the company's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is reevaluated annually, and tasks are incorporated into the regular Deal Engine product development process so they can be dealt with predictably and iteratively.

Integration with Risk Assessment

The environment in which the system operates, the commitments, agreements, and responsibilities of Deal Engine's system, as well as the nature of the components of the system, result in risks that the criteria will not be met. Deal Engine addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meet the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Deal Engine's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

CONTROL ACTIVITIES

Control activities are the actions established by policies and procedures to help ensure that management directives to mitigate risks to the achievement of objectives are executed. Control activities are performed at all levels of the organization and various stages within business processes, and over the technology environment.

INFORMATION AND COMMUNICATION SYSTEM

Information and communication are an integral component of Deal Engine'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.

Deal Engine uses several information and communication channels internally to share information with management, employees, contractors, and customers. Deal Engine uses chat systems and email as the primary internal and external communications channels.

Structured data is communicated internally via Software-as-a-Service (SaaS) applications and project management tools. Finally, Deal Engine uses in-person and video "all together" meetings to communicate company priorities and goals from management to all employees.

MONITORING CONTROLS

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

Ongoing Monitoring

Deal Engine's management conducts quality assurance monitoring on a regular basis, and additional training is provided based on the results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in Deal Engine's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Deal Engine's personnel.

Monitoring of the Subservice Organizations

Deal Engine uses multiple subservice organizations to provide cloud hosting services.

The management of Deal Engine receives and reviews the SOC 2 reports of AWS and GCP on an annual basis. In addition, through its daily operational activities, the management of Deal Engine monitors the services performed by AWS and GCP to ensure that operations and controls expected to be implemented at AWS and GCP are functioning effectively.

Reporting Deficiencies

Deal Engine's internal risk management tracking tool is utilized to document and track the results of ongoing monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool.

Annual risk meetings are held for management to review reported deficiencies and corrective actions.

CHANGES TO THE SYSTEM DURING THE PERIOD

No significant changes have occurred to the services provided to user entities during the examination period.

SYSTEM INCIDENTS DURING THE PERIOD

No significant system incidents have occurred to the services provided to user entities during the examination period.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS (CSOCs)

Deal Engine's controls related to the system cover only a portion of overall internal control for each user entity of Deal Engine. It is not feasible for the trust services criteria related to the system to be achieved solely by Deal Engine. Therefore, each user entity's internal controls should be evaluated in conjunction with Deal Engine's controls and the related tests and results described in Section 4 of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organizations as described below.

#	Complementary Subservice Organization Controls (CSOC)	Related Criteria
1	Amazon Web Services (AWS) and Google Cloud Platform (GCP) are responsible for maintaining physical security and environmental protection controls over the data centers hosting the Deal Engine infrastructure.	CC6.4
2	Amazon Web Services (AWS) and Google Cloud Platform (GCP) are responsible for the destruction of physical assets hosting the production environment.	CC6.5

COMPLEMENTARY USER ENTITY CONTROLS (CUECs)

Deal Engine's controls related to the Automated Refunds and Changes Platform only cover a portion of the overall internal controls for each user entity. It is not feasible for the applicable trust services criteria related to the system to be achieved solely by Deal Engine's control procedures. Accordingly, user entities, in conjunction with the services, should establish their internal controls or procedures to complement those of Deal Engine.

User auditors should determine whether the following controls have been in place in operation at the user organization:

1. User entities should have controls in place to provide reasonable assurance that user access including the provisioning and de-provisioning are designed appropriately and operating effectively.
2. User entities are responsible for reporting issues with Deal Engine systems and platforms.
3. User entities are responsible for understanding and complying with their contractual obligations to Deal Engine.
4. User entities are responsible for notifying Deal Engine of changes made to the administrative contact information.

TRUST SERVICES CATEGORY, CRITERIA, AND RELATED CONTROLS

The Security category and applicable trust services criteria were used to evaluate the suitability of the design of controls stated in the description. The criteria and controls designed, implemented, and operated to meet them ensure that information, systems, and access (physical and logical) are protected against unauthorized access, and systems are available for operation and use. The controls supporting the applicable trust services criteria are included in Section 4 of this report and are an integral part of the description of the system.

For specific criteria, which were deemed not relevant to the system, see Section 4 for the related explanation.

SECTION 4: TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS AND TESTS OF CONTROLS

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

This SOC 2 Type 2 report was prepared in accordance with the AICPA attestation standards and has been performed to examine the suitability of the design and operating effectiveness of controls to meet the criteria for the Security category set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*With Revised Points of Focus—2022)* in AICPA*, Trust Services Criteria* throughout the period September 1, 2024, to September 30, 2025.

The applicable trust services criteria and related controls specified by Deal Engine are presented in Section 4 of this report.

Test procedures performed in connection with determining the operating effectiveness of controls detailed here in Section 4 are described below:

- Inquiries – Inquiry of appropriate personnel and corroboration with management.
- Observation – Observation of the application, performance, or existence of the control.
- Inspection – Inspection of documents and reports indicating the performance of the control.
- Reperformance – Reperformance of the control.

FOOTNOTES FOR TEST RESULTS WHEN NO TESTS OF OPERATING EFFECTIVENESS WERE PERFORMED

1. The circumstances that warranted the operation of the control did not occur during the examination period; therefore, no tests of operating effectiveness were performed.

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	Controls	Detailed Tests of Controls	Test Results
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	The company performs background checks on new employees.	Inspected the completed background checks for a sample of new employees to determine that the company performed background checks on new employees.	No exceptions noted.
CC1.1.2	The company requires contractor agreements to include a code of conduct or reference to the company code of conduct.	Inspected the Code of Conduct acknowledgements for a sample of new contractors to determine that the company required contractor agreements to include a code of conduct or reference to the company's code of conduct.	No exceptions noted.
CC1.1.3	The company requires employees and contractors to acknowledge a Code of Conduct at the time of hire. Employees and contractors who violate the Code of Conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Inspected the acknowledgments of the Code of Conduct for a sample of new employees and contractors to determine that the Code of Conduct was acknowledged at the time of hire.	No exceptions noted.
		Per inquiry with management and inspection of the company’s code of conduct violation listing, there were no violations identified during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	Controls	Detailed Tests of Controls	Test Results
CC1.1.4	The company requires contractors to sign a confidentiality agreement at the time of engagement.	Inspected the signed Non-Disclosure Agreements (NDAs) for a sample of contractors to determine that the company required contractors to sign a confidentiality agreement at the time of engagement.	No exceptions noted.
CC1.1.5	The company requires employees to sign a confidentiality agreement during onboarding.	Inspected the signed NDAs for a sample of new employees to determine that the company required employees to sign a confidentiality agreement during onboarding.	No exceptions noted.
CC1.1.6	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected the completed performance evaluation for a sample of active employees to determine that the company's managers were required to complete performance evaluations for direct reports annually.	No exceptions noted.
CC1.2 - COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2.1	The company does not have an independent board of directors; therefore, this criterion is not applicable.		

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3.1	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy or job descriptions.	Inspected the company's Information Security Roles and Responsibilities Policy and the IT Manager job description to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in the Information Security Roles and Responsibilities Policy.	No exceptions noted.
CC1.3.2	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspected the Information Security Roles and Responsibilities Policy to determine that defined roles and responsibilities were established to oversee the design and implementation of information security controls.	No exceptions noted.
CC1.3.3	The company maintains an organizational chart that describes the organizational structure and reporting lines.	Inspected the company's organizational chart to determine that the company maintained an organizational chart that described the organizational structure and reporting lines.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy or job descriptions.	Inspected the company's Information Security Roles and Responsibilities Policy and the IT Manager job description to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in the Information Security Roles and Responsibilities Policy.	No exceptions noted.
CC1.4.2	The company performs background checks on new employees.	Inspected the completed background checks for a sample of new employees to determine that the company performed background checks on new employees.	No exceptions noted.
CC1.4.3	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected the completed performance evaluation for a sample of active employees to determine that the company's managers were required to complete performance evaluations for direct reports annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.4.4	The company requires employees to complete security awareness training within thirty days of hire and active employees to complete security awareness training at least annually.	Inspected the training records for a sample of new employees to determine that the company required employees to complete security awareness training within thirty days of hire.	No exceptions noted.
		Inspected the training records for a sample of active employees to determine that the company required employees to complete security awareness training at least annually.	No exceptions noted.
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy or job descriptions.	Inspected the company's Information Security Roles and Responsibilities Policy and the IT Manager job description to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in the Information Security Roles and Responsibilities Policy.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	Controls	Detailed Tests of Controls	Test Results
CC1.5.2	The company requires employees and contractors to acknowledge a Code of Conduct at the time of hire. Employees and contractors who violate the Code of Conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Inspected the acknowledgments of the Code of Conduct for a sample of new employees and contractors to determine that the Code of Conduct was acknowledged at the time of hire.	No exceptions noted.
		Per inquiry with management and inspection of the company's code of conduct violation listing, there were no violations identified during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.
CC1.5.3	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected the completed performance evaluation for a sample of active employees to determine that the company's managers were required to complete performance evaluations for direct reports annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
COMMUNICATION AND INFORMATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively.	Inspected the company's compliance platform to determine that the company performed control self-assessments at least annually to gain assurance that controls were in place and operating effectively.	No exceptions noted.
CC2.1.2	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Inspected the log management tool configurations to determine that the company utilized a log management tool to identify events that may potentially impact on the company's ability to achieve its security objectives.	No exceptions noted.
CC2.1.3	Host-based vulnerability scans are performed at least quarterly on all in-scope systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the vulnerability management configurations and the continuous scanning results to determine that vulnerability scans were performed quarterly on in-scope systems.	No exceptions noted.
		Inspected the vulnerability management dashboard and remediation records to determine that critical and high vulnerabilities were tracked to remediation.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
COMMUNICATION AND INFORMATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.2.1	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy or job descriptions.	Inspected the company's Information Security Roles and Responsibilities Policy and the IT Manager job description to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in the Information Security Roles and Responsibilities Policy.	No exceptions noted.
CC2.2.2	The company communicates system changes to authorized internal users via intranet/communication channel.	Inspected the company's internal communication channel to determine that the company communicated system changes to authorized internal users.	No exceptions noted.
CC2.2.3	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspected the Information Security Roles and Responsibilities Policy to determine that defined roles and responsibilities were established to oversee the design and implementation of information security controls.	No exceptions noted.
CC2.2.4	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were documented and reviewed annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
COMMUNICATION AND INFORMATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC2.2.5	The company has security incident response policies and procedures that are documented and communicated to authorized users via the compliance platform.	Inspected the company’s Incident Response Plan and the compliance platform to determine that the company had security incident response policies and procedures that were documented and communicated to authorized users via the compliance platform.	No exceptions noted.
CC2.2.6	The company provides a description of its products and services to internal and external users.	Inspected the company’s website to determine that the company provided a description of its products and services to internal and external users.	No exceptions noted.
CC2.2.7	The company requires employees to complete security awareness training within thirty days of hire and active employees to complete security awareness training at least annually.	Inspected the training records for a sample of new employees to determine that the company required employees to complete security awareness training within thirty days of hire.	No exceptions noted.
		Inspected the training records for a sample of active employees to determine that the company required employees to complete security awareness training at least annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
COMMUNICATION AND INFORMATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	The company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	Inspected the company’s website to determine that the company had contact information on their website to allow users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	No exceptions noted.
CC2.3.2	The company notifies customers of critical system changes that may affect their processing.	Inspected the company's website release notes to determine that the company notified customers of critical system changes that may affect their processing.	No exceptions noted.
CC2.3.3	The company’s security commitments are communicated to customers in the Terms and Conditions and Privacy Policy.	Inspected the company's Terms and Conditions and Privacy Policy to determine that the company’s security commitments were communicated to customers in the Terms and Conditions and Privacy Policy	No exceptions noted.
CC2.3.4	The company provides guidelines and technical support resources relating to system operations to customers.	Inspected the company’s website to determine that the company provided guidelines and technical support resources relating to system operations to customers.	No exceptions noted.
CC2.3.5	The company provides a description of its products and services to internal and external users.	Inspected the company’s website to determine that the company provided a description of its products and services to internal and external users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
COMMUNICATION AND INFORMATION			
Control Number	Controls	Detailed Tests of Controls	Test Results
CC2.3.6	The company has written agreements in place with vendors and related third parties. These agreements include security commitments applicable to that entity.	Inspected the Terms of Service for a sample of vendors to determine that security commitments were in place for vendors and related third parties.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**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.			
CC3.1.1	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively.	Inspected the company's compliance platform to determine that the company performed control self-assessments at least annually to gain assurance that controls were in place and operating effectively.	No exceptions noted.
CC3.1.2	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the company's Risk Management Policy and the completed security risk assessment to determine that the company specified its objectives to enable the identification and assessment of risk related to the objectives.	No exceptions noted.
CC3.1.3	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the company's Risk Management Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC3.1.4	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the completed security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to service commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
CC3.2 - COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC3.2.1	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests the business continuity/disaster recovery (BC/DR) plan at least annually.	Inspected the company’s BC/DR Plan to determine that the company had a documented BC/DR plan.	No exceptions noted.
		Inspected the company’s disaster recovery tabletop exercise meeting minutes to determine that the BC/DR plan was tested annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	Controls	Detailed Tests of Controls	Test Results
CC3.2.2	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the completed security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to service commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
CC3.2.3	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the company's Risk Management Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC3.2.4	The company has a third-party management program in place. Components of this program include: - critical vendor inventory; - vendors' security requirements; and - review of critical vendors at least annually.	Inspected the company's Third-Party Management Policy to determine that the company had a third-party management program in place that included the security requirements for vendors.	No exceptions noted.
		Inspected the company's vendor listing to determine that the critical vendor inventory was in place.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	Controls	Detailed Tests of Controls	Test Results
		Inspected the security review for a sample of critical vendors to determine that a review of critical vendors was performed annually.	No exceptions noted.
CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the completed security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to service commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
CC3.3.2	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the company's Risk Management Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate critical and high vulnerabilities in accordance with SLAs.	Inspected the company's third-party penetration test report results to determine that penetration testing was performed at least annually.	No exceptions noted.
		Per inquiry with management and inspection of the penetration test report, it was noted that there were no critical or high-risk vulnerabilities found in the report; therefore, no testing was performed.	No testing performed. See footnote 1 above.
CC3.4.2	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the completed security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to service commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	Controls	Detailed Tests of Controls	Test Results
CC3.4.3	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the company’s Risk Management Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC3.4.4	The company has a third-party management program in place. Components of this program include: - critical vendor inventory; - vendors' security requirements; and - review of critical vendors at least annually.	Inspected the company’s Third-Party Management Policy to determine that the company had a third-party management program in place that included the security requirements for vendors.	No exceptions noted.
		Inspected the company's vendor listing to determine that the critical vendor inventory was in place.	No exceptions noted.
		Inspected the security review for a sample of critical vendors to determine that a review of critical vendors was performed annually.	No exceptions noted.
CC3.4.5	Host-based vulnerability scans are performed at least quarterly on all in-scope systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the vulnerability management configurations and the continuous scanning results to determine that vulnerability scans were performed quarterly on in-scope systems.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	Controls	Detailed Tests of Controls	Test Results
		Inspected the vulnerability management dashboard and remediation records to determine that critical and high vulnerabilities were tracked to remediation.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
MONITORING ACTIVITIES			
Control Number	Controls	Detailed Tests of Controls	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.			
CC4.1.1	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively.	Inspected the company's compliance platform to determine that the company performed control self-assessments at least annually to gain assurance that controls were in place and operating effectively.	No exceptions noted.
CC4.1.2	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate critical and high vulnerabilities in accordance with SLAs.	Inspected the company's third-party penetration test report results to determine that penetration testing was performed at least annually.	No exceptions noted.
		Per inquiry with management and inspection of the penetration test report, it was noted that there were no critical or high-risk vulnerabilities found in the report; therefore, no testing was performed.	No testing performed. See footnote 1 above.
CC4.1.3	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the completed security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to service commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
MONITORING ACTIVITIES			
Control Number	Controls	Detailed Tests of Controls	Test Results
CC4.1.4	The company has a third-party management program in place. Components of this program include: - critical vendor inventory; - vendors' security requirements; and - review of critical vendors at least annually.	Inspected the company’s Third-Party Management Policy to determine that the company had a third-party management program in place that included the security requirements for vendors.	No exceptions noted.
		Inspected the company's vendor listing to determine that the critical vendor inventory was in place.	No exceptions noted.
		Inspected the security review for a sample of critical vendors to determine that a review of critical vendors was performed annually.	No exceptions noted.
CC4.1.5	Host-based vulnerability scans are performed at least quarterly on all in-scope systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the vulnerability management configurations and the scan results to determine that vulnerability scans were performed quarterly on in-scope systems.	No exceptions noted.
		Inspected the vulnerability management dashboard and remediation records to determine that critical and high vulnerabilities were tracked to remediation.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
MONITORING ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
CC4.2.1	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively.	Inspected the company’s compliance platform to determine that the company performed control self-assessments at least annually to gain assurance that controls were in place and operating effectively.	No exceptions noted.
CC4.2.2	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate critical and high vulnerabilities in accordance with SLAs.	Inspected the company's third-party penetration test report results to determine that penetration testing was performed at least annually.	No exceptions noted.
		Per inquiry with management and inspection of the penetration test report, it was noted that there were no critical or high-risk vulnerabilities found in the report; therefore, no testing was performed.	No testing performed. See footnote 1 above.
CC4.2.3	The company's security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the supporting remediation documentation for a sample of incidents to determine that the company’s security incidents were logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company’s security incident response policy and procedures.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
MONITORING ACTIVITIES			
Control Number	Controls	Detailed Tests of Controls	Test Results
CC4.2.4	The company has a third-party management program in place. Components of this program include: - critical vendor inventory; - vendors' security requirements; and - review of critical vendors at least annually.	Inspected the company's Third-Party Management Policy to determine that the company had a third-party management program in place that included the security requirements for vendors.	No exceptions noted.
		Inspected the company's vendor listing to determine that the critical vendor inventory was in place.	No exceptions noted.
		Inspected the security review for a sample of critical vendors to determine that a review of critical vendors was performed annually.	No exceptions noted.
CC4.2.5	Host-based vulnerability scans are performed at least quarterly on all in-scope systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the vulnerability management configurations and the scan results to determine that vulnerability scans were performed quarterly on in-scope systems.	No exceptions noted.
		Inspected the vulnerability management dashboard and remediation records to determine that critical and high vulnerabilities were tracked to remediation.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**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.			
CC5.1.1	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy or job descriptions.	Inspected the company's Information Security Roles and Responsibilities Policy and the IT Manager job description to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in the Information Security Roles and Responsibilities Policy.	No exceptions noted.
CC5.1.2	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were documented and reviewed annually.	No exceptions noted.
CC5.1.3	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively.	Inspected the company's compliance platform to determine that the company performed control self-assessments at least annually to gain assurance that controls were in place and operating effectively.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	Controls	Detailed Tests of Controls	Test Results
CC5.1.4	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the company's Risk Management Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC5.1.5	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the completed security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to service commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the company's Secure Development Policy to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.
		Inspected the change management documentation for a sample of changes to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.
CC5.2.2	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's Operations Security and Secure Development policies to determine that the company had a formal SDLC methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC5.2.3	The company’s information security policies and procedures are documented and reviewed at least annually.	Inspected the company’s information security policies and procedures to determine that the company’s information security policies and procedures were documented and reviewed annually.	No exceptions noted.
CC5.2.4	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the company’s Access Control Policy to determine that the Access Control Policy documented the requirements for adding, modifying, and removing user access.	No exceptions noted.
CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the company’s Secure Development Policy to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	Controls	Detailed Tests of Controls	Test Results
		Inspected the change management documentation for a sample of changes to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.
CC5.3.2	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's Operations Security and Secure Development policies to determine that the company had a formal SDLC methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.
CC5.3.3	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy or job descriptions.	Inspected the company's Information Security Roles and Responsibilities Policy and the IT Manager job description to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in the Information Security Roles and Responsibilities Policy.	No exceptions noted.

<table>
<tr><th colspan="4">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="4">CONTROL ACTIVITIES</th></tr>
<tr><th>Control Number</th><th>Controls</th><th>Detailed Tests of Controls</th><th>Test Results</th></tr>
<tr><td>CC5.3.4</td><td>The company’s information security policies and procedures are documented and reviewed at least annually.</td><td>Inspected the company’s information security policies and procedures to determine that the company’s information security policies and procedures were documented and reviewed annually.</td><td>No exceptions noted.</td></tr>
<tr><td>CC5.3.5</td><td>The company specifies its objectives to enable the identification and assessment of risk related to the objectives.</td><td>Inspected the company’s Risk Management Policy and the completed security risk assessment to determine that the company specified its objectives to enable the identification and assessment of risk related to the objectives.</td><td>No exceptions noted.</td></tr>
<tr><td>CC5.3.6</td><td>The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.</td><td>Inspected the company’s Risk Management Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.</td><td>No exceptions noted.</td></tr>
</table>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	Controls	Detailed Tests of Controls	Test Results
CC5.3.7	The company has a third-party management program in place. Components of this program include: - critical vendor inventory; - vendors' security requirements; and - review of critical vendors at least annually.	Inspected the company’s Third-Party Management Policy to determine that the company had a third-party management program in place that included the security requirements for vendors.	No exceptions noted.
		Inspected the company's vendor listing to determine that the critical vendor inventory was in place.	No exceptions noted.
		Inspected the security review for a sample of critical vendors to determine that a review of critical vendors was performed annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**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.			
CC6.1.1	The company maintains a formal inventory of production system assets.	Inspected the company's inventory listing of information assets to determine that the company maintained a formal inventory of production system assets.	No exceptions noted.
CC6.1.2	The company's datastores housing sensitive customer data are encrypted at rest.	Inspected the encryption configurations for data at rest to determine that the company's datastores housing sensitive customer data were encrypted at rest.	No exceptions noted.
CC6.1.3	The company has a Data Management Policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the company’s Data Management Policy to determine that the company had a Data Management Policy in place to help ensure that confidential data was properly secured and restricted to authorized personnel.	No exceptions noted.
CC6.1.4	Access to production applications, servers, and databases is restricted to authorized users with a business need.	Inspected the administrator user listing and access roles to determine that access to production applications, servers, and databases was restricted to authorized users with a business need.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.1.5	The company restricts administrative access to system components to only authorized personnel (network, networking devices, database, operating system, application, encryption keys, moving changes to production).	Inspected the administrator user listing for the in-scope system components to determine that administrative access was limited to only authorized personnel.	No exceptions noted.
CC6.1.6	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the password and authentication configurations, and the complete user listing and access roles for the production networks to determine that unique usernames and passwords or authorized Secure Socket Shell (SSH) keys were utilized to access the production network.	No exceptions noted.
CC6.1.7	The company requires passwords for in-scope system components to be configured according to the company's policy.	Inspected the password configurations and written password policy to determine that the company required passwords for in-scope system components to be configured according to the company’s policy.	Exceptions noted: The password parameters for the company-developed application were not configured to comply with the company's corporate password policy.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.1.8	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the company's Infrastructure as a Service provider's TLS certificate to determine that the company's production systems could only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
CC6.1.9	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the company's Access Control Policy to determine that the Access Control Policy documented the requirements for adding, modifying, and removing user access.	No exceptions noted.
CC6.1.10	The company ensures that user access to in-scope system components is based on job role and function.	Inspected the access provisioning documentation for a sample of new contractors and employees to determine that the company ensured that user access to in-scope system components was based on job role and function.	No exceptions noted.
CC6.1.11	The company's network is segmented to prevent unauthorized access to customer data.	Inspected the network configurations for the in-scope environments to determine that the company's network was segmented to prevent unauthorized access to customer data.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC6.2.1	The company conducts access reviews on a quarterly basis for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the logical user access review documentation for a sample of quarters to determine that the company conducted quarterly access reviews for the in-scope system components to help ensure that access was restricted appropriately.	No exceptions noted.
CC6.2.2	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the company’s Access Control Policy to determine that the Access Control Policy documented the requirements for adding, modifying, and removing user access.	No exceptions noted.
CC6.2.3	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the user access revocation documentation for a sample of terminated employees to determine that logical access to systems was revoked as a component of the termination process within the company’s SLAs.	No exceptions noted.
CC6.2.4	The company ensures that user access to in-scope system components is based on job role and function.	Inspected the access provisioning documentation for a sample of new contractors and employees to determine that the company ensured that user access to in-scope system components was based on job role and function.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	Controls	Detailed Tests of Controls	Test Results
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
CC6.3.1	The company conducts access reviews on a quarterly basis for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the logical user access review documentation for a sample of quarters to determine that the company conducted quarterly access reviews for the in-scope system components to help ensure that access was restricted appropriately.	No exceptions noted.
CC6.3.2	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the company's Access Control Policy to determine that the Access Control Policy documented the requirements for adding, modifying, and removing user access.	No exceptions noted.
CC6.3.3	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the user access revocation documentation for a sample of terminated employees to determine that logical access to systems was revoked as a component of the termination process within the company's SLAs.	No exceptions noted.
CC6.3.4	The company ensures that user access to in-scope system components is based on job role and function.	Inspected the access provisioning documentation for a sample of new contractors and employees to determine that the company ensured that user access to in-scope system components was based on job role and function.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
CC6.4.1	Management contracts with AWS and GCP to provide physical access security for its production systems.	This control activity is the responsibility of the subservice organizations. Refer to the Subservice Organizations section above for controls managed by the subservice organizations.	
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
CC6.5.1	The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.	Inspected the media disposal records for a sample of devices to determine that the company had electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction were issued for each device destroyed.	No exceptions noted.
CC6.5.2	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the data disposal and retention procedures to determine that the company had formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	No exceptions noted.
CC6.5.3	The destruction of physical assets hosting the production environment is the responsibility of AWS and GCP.	This control activity is the responsibility of the subservice organizations. Refer to the Subservice Organizations section above for controls managed by the subservice organizations.	

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the company's Infrastructure as a Service provider's TLS certificate to determine that the company's production systems could only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
CC6.6.2	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the IDS configurations for the in-scope system components to determine that the company used an IDS to provide continuous monitoring of the company's network and early detection of potential security breaches.	No exceptions noted.
CC6.6.3	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the company's website and TLS certificate to determine that the company used secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	No exceptions noted.
CC6.6.4	The company reviews its firewall rulesets at least annually. Required changes are tracked to completion.	Inspected the company's firewall ruleset review documentation to determine that the company reviewed its firewall rulesets at least annually and that required changes were tracked to completion.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.6.5	The company uses firewalls and configures them to prevent unauthorized access.	Inspected the firewall ruleset configurations to determine that the firewall was configured to prevent unauthorized access to the company’s network.	No exceptions noted.
CC6.6.6	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Inspected the Operations Security Policy to determine that standards were documented based on industry best practices and reviewed at least annually.	No exceptions noted.
CC6.6.7	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the vulnerability management configurations and the continuous scanning results to determine that the company had infrastructure supporting the service patched as part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service were hardened against security threats.	No exceptions noted.
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
CC6.7.1	The company encrypts portable devices when used.	Inspected the encryption configurations for a sample of devices to determine that the company encrypted portable media devices when used.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.7.2	The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.	Inspected the company’s MDM system to determine that the company had an MDM system in place to centrally monitor mobile devices supporting the service.	No exceptions noted.
CC6.7.3	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the company’s website and TLS certificate to determine that the company used secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	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.			
CC6.8.1	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company’s Operations Security and Secure Development policies to determine that the company had a formal SDLC methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.
CC6.8.2	The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.	Inspected the anti-malware configurations for a sample of workstations to determine that anti-malware technology was deployed, routinely updated, logged, and installed on all relevant systems.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.8.3	The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.	Inspected the company's MDM system to determine that the company had an MDM system in place to centrally monitor mobile devices supporting the service.	No exceptions noted.
CC6.8.4	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the vulnerability management configurations and the continuous scanning results to determine that the company had infrastructure supporting the service patched as part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service were hardened against security threats.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**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.			
CC7.1.1	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected the company's Operations Security Policy to determine that the company had a configuration management procedure in place to ensure that system configurations were deployed consistently throughout the environment.	No exceptions noted.
CC7.1.2	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the company's Secure Development Policy to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.
		Inspected the change management documentation for a sample of changes to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	Controls	Detailed Tests of Controls	Test Results
CC7.1.3	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Inspected the log management tool configurations to determine that the company utilized a log management tool to identify events that may potentially impact the company’s ability to achieve its security objectives.	No exceptions noted.
CC7.1.4	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Inspected the company’s Operations Security Policy to determine that the company’s formal policies outlined the requirements for the following IT/Engineering functions including vulnerability management and system monitoring.	No exceptions noted.
CC7.1.5	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the completed security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to service commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	Controls	Detailed Tests of Controls	Test Results
CC7.1.6	Host-based vulnerability scans are performed at least quarterly on all in-scope systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the vulnerability management configurations and the scan results to determine that vulnerability scans were performed quarterly on in-scope systems.	No exceptions noted.
		Inspected the vulnerability management dashboard and remediation records to determine that critical and high vulnerabilities were tracked to remediation.	No exceptions noted.
CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC7.2.1	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate critical and high vulnerabilities in accordance with SLAs.	Inspected the company's third-party penetration test report results to determine that penetration testing was performed at least annually.	No exceptions noted.
		Per inquiry with management and inspection of the penetration test report, it was noted that there were no critical or high-risk vulnerabilities found the report; therefore, no testing was performed.	No testing performed. See footnote 1 above.
CC7.2.2	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the IDS configurations for the in-scope system components to determine that the company used an IDS to provide continuous monitoring of the company’s network and early detection of potential security breaches.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	Controls	Detailed Tests of Controls	Test Results
CC7.2.3	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Inspected the log management tool configurations to determine that the company utilized a log management tool to identify events that may potentially impact the company's ability to achieve its security objectives.	No exceptions noted.
CC7.2.4	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Inspected the monitoring tool configurations to determine that an infrastructure monitoring tool was utilized to monitor systems, infrastructure, and performance, and generated alerts when specific predefined thresholds were met.	No exceptions noted.
CC7.2.5	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Inspected the company's Operations Security Policy to determine that the company's formal policies outlined the requirements for the following IT/Engineering functions including vulnerability management and system monitoring.	No exceptions noted.
CC7.2.6	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the vulnerability management configurations and the continuous scanning results to determine that the company had infrastructure supporting the service patched as part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service were hardened against security threats.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	Controls	Detailed Tests of Controls	Test Results
CC7.2.7	Host-based vulnerability scans are performed at least quarterly on all in-scope systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the vulnerability management configurations and the scan results to determine that vulnerability scans were performed quarterly on in-scope systems.	No exceptions noted.
		Inspected the vulnerability management dashboard and remediation records to determine that critical and high vulnerabilities were tracked to remediation.	No exceptions noted.
CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.3.1	The company has security incident response policies and procedures that are documented and communicated to authorized users via the compliance platform.	Inspected the company's Incident Response Plan and the compliance platform to determine that the company had security incident response policies and procedures that were documented and communicated to authorized users via the compliance platform.	No exceptions noted.
CC7.3.2	The company's security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the supporting remediation documentation for a sample of incidents to determine that the company's security incidents were logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.4 - The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.4.1	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate critical and high vulnerabilities in accordance with SLAs.	Inspected the company's third-party penetration test report results to determine that penetration testing was performed at least annually.	No exceptions noted.
		Per inquiry with management and inspection of the penetration test report, it was noted that there were no critical or high-risk vulnerabilities found in the report; therefore, no testing was performed.	No testing performed. See footnote 1 above.
CC7.4.2	The company has an incident response plan in place and tests their incident response plan at least annually.	Inspected the company's disaster recovery tabletop exercise meeting minutes, including the incident response plan, to determine that the company tested its incident response plan at least annually.	No exceptions noted.
CC7.4.3	The company has security incident response policies and procedures that are documented and communicated to authorized users via the compliance platform.	Inspected the company's Incident Response Plan and the compliance platform to determine that the company had security incident response policies and procedures that were documented and communicated to authorized users via the compliance platform.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	Controls	Detailed Tests of Controls	Test Results
CC7.4.4	The company's security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the supporting remediation documentation for a sample of incidents to determine that the company’s security incidents were logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company’s security incident response policy and procedures.	No exceptions noted.
CC7.4.5	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the vulnerability management configurations and the continuous scanning results to determine that the company had infrastructure supporting the service patched as part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service were hardened against security threats.	No exceptions noted.
CC7.4.6	Host-based vulnerability scans are performed at least quarterly on all in-scope systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the vulnerability management configurations and the scan results to determine that vulnerability scans were performed quarterly on in-scope systems.	No exceptions noted.
		Inspected the vulnerability management dashboard and remediation records to determine that critical and high vulnerabilities were tracked to remediation.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests the business continuity/disaster recovery (BC/DR) plan at least annually.	Inspected the company's BC/DR Plan to determine that the company had a documented BC/DR plan.	No exceptions noted.
		Inspected the company's disaster recovery tabletop exercise meeting minutes to determine that the BC/DR plan was tested annually.	No exceptions noted.
CC7.5.2	The company has an incident response plan in place and tests their incident response plan at least annually.	Inspected the company's disaster recovery tabletop exercise meeting minutes, including the incident response plan, to determine that the company tested its incident response plan at least annually.	No exceptions noted.
CC7.5.3	The company has security incident response policies and procedures that are documented and communicated to authorized users via the compliance platform.	Inspected the company's Incident Response Plan and the compliance platform to determine that the company had security incident response policies and procedures that were documented and communicated to authorized users via the compliance platform.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	Controls	Detailed Tests of Controls	Test Results
CC7.5.4	The company's security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the supporting remediation documentation for a sample of incidents to determine that the company’s security incidents were logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company’s security incident response policy and procedures.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CHANGE MANAGEMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**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.			
CC8.1.1	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the company's Secure Development Policy to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.
		Inspected the change management documentation for a sample of changes to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.
CC8.1.2	The company restricts access to migrate changes to production to authorized personnel.	Inspected the branch protection rule configurations and the users with the ability to deploy changes to the production environment to determine that the company restricted access to migrate changes to production to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CHANGE MANAGEMENT			
Control Number	Controls	Detailed Tests of Controls	Test Results
CC8.1.3	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's Operations Security and Secure Development policies to determine that the company had a formal SDLC methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.
CC8.1.4	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate critical and high vulnerabilities in accordance with SLAs.	Inspected the company's third-party penetration test report results to determine that penetration testing was performed at least annually.	No exceptions noted.
		Per inquiry with management and inspection of the penetration test report, it was noted that there were no critical or high-risk vulnerabilities found in the report; therefore, no testing was performed.	No testing performed. See footnote 1 above.
CC8.1.5	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Inspected the Operations Security Policy to determine that standards were documented based on industry best practices and reviewed at least annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CHANGE MANAGEMENT			
Control Number	Controls	Detailed Tests of Controls	Test Results
CC8.1.6	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the vulnerability management configurations and the continuous scanning results to determine that the company had infrastructure supporting the service patched as part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service were hardened against security threats.	No exceptions noted.
CC8.1.7	Host-based vulnerability scans are performed at least quarterly on all in-scope systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the vulnerability management configurations and the scan results to determine that vulnerability scans were performed quarterly on in-scope systems.	No exceptions noted.
		Inspected the vulnerability management dashboard and remediation records to determine that critical and high vulnerabilities were tracked to remediation.	No exceptions noted.

<table>
<tr><th colspan="4">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="4">RISK MITIGATION</th></tr>
<tr><th>Control Number</th><th>Controls</th><th>Detailed Tests of Controls</th><th>Test Results</th></tr>
<tr><td colspan="4"><b>CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.</b></td></tr>
<tr><td>CC9.1.1</td><td>The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.</td><td>Inspected the Business Continuity and Disaster Recovery Plan to determine that communication plans were clearly outlined to maintain information security continuity in the event of the unavailability of key personnel.</td><td>No exceptions noted.</td></tr>
<tr><td>CC9.1.2</td><td>The company maintains cybersecurity insurance to mitigate the financial impact of business disruptions.</td><td>Inspected the cybersecurity insurance documentation to determine that the company maintained adequate coverage to mitigate the financial impact of business disruptions.</td><td>No exceptions noted.</td></tr>
<tr><td>CC9.1.3</td><td>The company has an incident response plan in place and tests their incident response plan at least annually.</td><td>Inspected the company’s disaster recovery tabletop exercise meeting minutes, including the incident response plan, to determine that the company tested its incident response plan at least annually.</td><td>No exceptions noted.</td></tr>
</table>

<table>
<tr><th colspan="4">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="4">RISK MITIGATION</th></tr>
<tr><th>Control Number</th><th>Controls</th><th>Detailed Tests of Controls</th><th>Test Results</th></tr>
<tr><td>CC9.1.4</td><td>The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.</td><td>Inspected the completed security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to service commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.</td><td>No exceptions noted.</td></tr>
<tr><td>CC9.1.5</td><td>The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.</td><td>Inspected the company’s Risk Management Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.</td><td>No exceptions noted.</td></tr>
<tr><td colspan="4"><b>CC9.2 - The entity assesses and manages risks associated with vendors and business partners.</b></td></tr>
<tr><td>CC9.2.1</td><td>The company has written agreements in place with vendors and related third parties. These agreements include security commitments applicable to that entity.</td><td>Inspected the Terms of Service for a sample of vendors to determine that security commitments were in place for vendors and related third parties.</td><td>No exceptions noted.</td></tr>
</table>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK MITIGATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC9.2.2	The company has a third-party management program in place. Components of this program include: - critical vendor inventory; - vendors' security requirements; and - review of critical vendors at least annually.	Inspected the company’s Third-Party Management Policy to determine that the company had a third-party management program in place that included the security requirements for vendors.	No exceptions noted.
		Inspected the company's vendor listing to determine that the critical vendor inventory was in place.	No exceptions noted.
		Inspected the security review for a sample of critical vendors to determine that a review of critical vendors was performed annually.	No exceptions noted.

SECTION 5:
OTHER INFORMATION PROVIDED BY DEAL ENGINE, INC.

MANAGEMENT’S RESPONSES TO THE NOTED EXCEPTIONS

Control Activity	Noted Exceptions	Management’s Responses
The company requires passwords for in-scope system components to be configured according to the company's policy.	Exceptions noted: The password parameters for the company-developed application were not configured to comply with the company's corporate password policy.	Management acknowledges the exception noted regarding the misalignment between the password settings of the company-developed application and the requirements outlined in the company’s password policy. Upon identification of the issue, the application’s configuration was updated to fully comply with the established policy. The remediation has been completed, and the control is now operating in accordance with requirements.