A-LIGN

Fin Technologies, Inc. dba Mantl

Type 2 SOC 2

2023

MANTL

REPORT ON FIN TECHNOLOGIES, INC. DBA MANTL'S DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY

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

April 1, 2022 to March 31, 2023

Table of Contents

SECTION 1

ASSERTION OF FIN TECHNOLOGIES, INC. DBA MANTL MANAGEMENT

ASSERTION OF FIN TECHNOLOGIES, INC. DBA MANTL MANAGEMENT

April 12, 2023

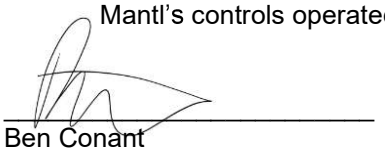
We have prepared the accompanying description of Fin Technologies, Inc. dba Mantl's ('Mantl' or 'the Company') Financial Software-as-a-Service Platform Services System titled "Fin Technologies, Inc. dba Mantl's Description of Its Financial Software-as-a-Service Platform Services System throughout the period April 1, 2022 to March 31, 2023" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the Financial Software-as-a-Service Platform Services System that may be useful when assessing the risks arising from interactions with Mantl's system, particularly information about system controls that Mantl 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, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Mantl uses Alloy to provide KYC/AML identity verification services, First Data to provide credit card processing and payment services, Google Cloud Platform ('GCP') to provide cloud hosting services, Plaid to provide banking data API system services and SendGrid to provide transactional and marketing email platform services (collectively, the 'subservice organizations'). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Mantl, to achieve Mantl's service commitments and system requirements based on the applicable trust services criteria. The description presents Mantl's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Mantl'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 Mantl, to achieve Mantl's service commitments and system requirements based on the applicable trust services criteria. The description presents Mantl's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Mantl's controls.

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

a. the description presents Mantl's Financial Software-as-a-Service Platform Services System that was designed and implemented throughout the period April 1, 2022 to March 31, 2023, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period April 1, 2022 to March 31, 2023, to provide reasonable assurance that Mantl'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 Mantl's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period April 1, 2022 to March 31, 2023, to provide reasonable assurance that Mantl'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 Mantl's controls operated effectively throughout that period.



Ben Conant
Chief Technology Officer
Fin Technologies, Inc. dba Mantl

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Fin Technologies, Inc. dba Mantl

Scope

We have examined Mantl's accompanying description of its Financial Software-as-a-Service Platform Services System titled "Fin Technologies, Inc. dba Mantl's Description of Its Financial Software-as-a-Service Platform Services System throughout the period April 1, 2022 to March 31, 2023" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period April 1, 2022 to March 31, 2023, to provide reasonable assurance that Mantl's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Mantl uses Alloy to provide KYC/AML identity verification services, First Data to provide credit card processing and payment services, GCP to provide cloud hosting services, Plaid to provide banking data API system services and SendGrid to provide transactional and marketing email platform services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Mantl, to achieve Mantl's service commitments and system requirements based on the applicable trust services criteria. The description presents Mantl's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Mantl'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 Mantl, to achieve Mantl's service commitments and system requirements based on the applicable trust services criteria. The description presents Mantl's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Mantl's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

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

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

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

Independence and Ethical Responsibilities

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

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

Description of Tests of Controls

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

Opinion

In our opinion, in all material respects,

a. the description presents Mantl's Financial Software-as-a-Service Platform Services System that was designed and implemented throughout the period April 1, 2022 to March 31, 2023, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period April 1, 2022 to March 31, 2023, to provide reasonable assurance that Mantl'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 Mantl's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period April 1, 2022 to March 31, 2023, to provide reasonable assurance that Mantl'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 Mantl'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 Mantl, user entities of Mantl's Financial Software-as-a-Service Platform Services System during some or all of the period April 1, 2022 to March 31, 2023, business partners of Mantl subject to risks arising from interactions with the Financial Software-as-a-Service Platform Services System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

A-LIGN ASSURANCE

Tampa, Florida
April 12, 2023

SECTION 3

FIN TECHNOLOGIES, INC. DBA MANTL'S DESCRIPTION OF ITS FINANCIAL SOFTWARE-AS-A-SERVICE PLATFORM SERVICES SYSTEM THROUGHOUT THE PERIOD APRIL 1, 2022 TO MARCH 31, 2023

OVERVIEW OF OPERATIONS

Company Background

Fin Technologies, Inc. dba Mantl is a customer-centric outer core ecosystem that gives banks and credit unions the flexibility to innovate using modern technology, while owning their brand throughout the entire customer lifecycle.

In their collective experience building everything from modern consumer FinTech companies to core banking systems, they saw a rift where new FinTech companies were able to leverage the latest technologies, while banks and credit unions - tethered to their outdated systems and vendors - struggled to remain competitive in the digital age.

That divide continues today. So, they pulled together a team with deep industry knowledge, and expertise in systems architecture, UI/UX, and data security and analysis to reunite the worlds of banking and technology.

Mantl was part of the Techstars' NYC Summer 2016 program and is Venture Capital-backed with corporate headquarters in New York City, New York.

Description of Services Provided

Mantl (mantl.com) provides a Software-as-a-Service (SaaS) platform that integrates services across financial institutions and provides customized application solutions for banks and credit unions of all sizes.

Principal Service Commitments and System Requirements

Mantl designs its processes and procedures to meet its objectives for its Financial Software-as-a-Service platform. Those objectives are based on the service commitments that Mantl makes to user entities, the laws and regulations that govern the provision of Financial Software-as-a-Service services, and the financial, operational, and compliance requirements that Mantl has established for the services.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security concepts within the fundamental designs of the Financial Software-as-a-Service platform that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role
- Use of encryption technologies to protect customer data both at rest and in transit

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

Components of the System

Infrastructure

Mantl hosts its application on the Google Cloud Platform (GCP) managed infrastructure. GCP owns and manages all the resources and assets associated with the infrastructure. Mantl manages the software code which is the end user application installed on GCP resources.

Primary infrastructure used to provide Fin Technologies, Inc. dba Mantl's Financial Software-as-a-Service Platform Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Web Servers	Docker containers running on Google Kubernetes engine with nginx ingress	Hosts files to support the web application and transaction server
Databases	Google Cloud PostgreSQL, Google Firestore, BigQuery	Stores encrypted database data to support the web application and transaction server
Firewalls	Cloud Armor and Cloudflare	Filters traffic into and out of the private network supporting the application services
Switches	GCP Managed	Connects devices on the corporate network by sending message to the specific device(s) that need to receive it
Routers	GCP Managed	Connects multiple networks and forward packets within the network or other networks

Software

Primary software used to provide Fin Technologies, Inc. dba Mantl's Financial Software-as-a-Service Platform Services System includes the following:

Primary Software	
Software	**Purpose**
Google Cloud Storage	Perform scheduled backups of client data according to the requirements defined by the customer and provides status alerts to operations personnel
Cloudflare	Web application firewall and Domain Name System (DNS)
Google Cloud Storage	Storage
Orca Security Platform	Monitoring application used to provide monitoring, alert, and notification services for the hosted client environments
GCP Identity and Access Management (IAM) and strongDM	Provides user administration including access control policies for authentication of users, commands, and audit logging
GIT	Version control software
Jira	Provides ticketing functionality to document and track issues and requests for the client environment

Primary Software	
Software	**Purpose**
Slack	Monitoring for alerts such as file integrity, security, availability
CrowdStrike	Antivirus
JAMF	Apple mobile device management
LogDNA	Application log management and analysis tool
Buildkite	Continuous integration/continuous delivery (CI/CD) pipeline tool
Okta	IAM and single sign-on (SSO)
Terraform	Infrastructure as code
Vault	Storing token, passwords, certificates, encryption keys
Auth0	Authentication and authorization service to access applications
BetterCloud	Onboarding and offboarding
1Password	Password manager
Greenhouse	Applicant tracking system and recruiting software
Gsuite	Email and Google apps
Orca Security	Infrastructure security monitoring
Dropbox	File storage

People

The Mantl staff provide support for the above service in each of the following functional areas:

- Chief Executive Officer (CEO) - Development and mission accomplishment
- Chief Technology Officer (CTO) - Planning, budgeting, and performance including information security
- Director of Engineering - Confidentiality, integrity, and availability of the IT systems and data
- Core Integration Architect - Core integration
- Software Engineers - Development and testing

Data

The Mantl Production environment is ensuring 256-bit Secure Socket Layer (SSL) encryption of all data in transit. Customer personally identifiable information (PII) will specifically be located and encrypted at rest within the relevant data tables using Advanced Encryption Standard 256 (AES 256) managed by Google Cloud PostgreSQL, Google Firestore, and BigQuery.

Processes, Policies and Procedures

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

Physical Security

The Mantl corporate headquarters in San Francisco, California requires an authorized badge to access both the building entry and again to gain access to the office. The office remains locked after business hours, and no equipment is left unattended even after hours.

Management performs monthly access reviews to validate that all persons with physical and logical access are active employees, and termination procedures applied ensure the timely retrieval of physical keys.

The physical security of the production servers is the responsibility of GCP. Refer to the "Subservice Organizations" section below for the controls in place around physical security.

Logical Access

Mantl uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Employee access to the GCP environment is controlled, by role, via the strongDM authentication. User, role-based, access is controlled in the application and authenticates to the database.

Additionally, Mantl uses Cloud IAM, where permissions to access a resource are grouped into roles. Roles are assigned to authenticated members. The Cloud IAM Policy classifies and defines roles assigned to individual members, and when an authenticated member accesses a resource, Cloud IAM verifies against the resource's roles to determine whether the action is valid and permitted.

Access to Kubernetes and database are routed through strongDM based on time-based approvals.

Passwords must conform to defined, complex, password standards and are enforced through parameter settings in the application.

Remote access into the production environment is tightly restricted to only authorized workers based on their role.

On a monthly basis, managers perform access reviews for workers with access to privileged roles and requests modifications based on least-privilege.

Computer Operations - Backups

Mantl replicates its application and database across two separate data centers within the GCP environment. In addition, full data backups are performed nightly. Applications deployed to the GCP platform are automatically backed up as part of the managed services process on secure, access controlled, and redundant storage.

As noted above, data is spread across data center locations within GCP. Nightly backups are retained for specified intervals, and failure alerts are received by the Director of Engineering and his designees. Failed backups are investigated and resolved in a timely manner.

Mantl utilizes continuous monitoring tools with alerting enabled to assess system health and data throughput which would signal if there were backup system issues. In addition, Management reviews the testing performed by independent auditors, as documented in Section 4 of the GCP annual SOC 2 report, to validate the operating effectiveness of the GCP backup and recovery controls.

Computer Operations - Availability

Mantl has implemented an Incident Response policy and procedures to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents.

Mantl monitors the capacity utilization of physical and computing infrastructure to ensure that service delivery matches service level agreements by monitoring the GCP Dashboard, related metrics, and alerts. Mantl evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers.

Mantl utilizes the vendor alerts, GCP Dashboard, Cloudflare, Orca Security Platform for System Metrics health tool to monitor the firewall, application and database servers and infrastructure routers and switches. Packets per second and CPU Load are monitored on the network along with the servers' memory usage, RAM, and disk space.

Change Control

Mantl maintains documented Infrastructure and Code Change Development 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 results, whenever applicable, 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. The Code Climate toolset is run against every code deployment to identify potential code vulnerabilities.

Infrastructure changes are performed by Mantl's infrastructure as a service provider, GCP, who houses the Mantl production environment within GCP data center locations. GCP is responsible for applying firmware and security patches; however, Mantl actively monitors vendor and security industry vulnerability notifications impacting its infrastructure servers, routers, databases, and operating systems to ensure timely patching by GCP personnel. In addition, Management will review the testing performed by independent auditors, as documented in Section 4 of the GCP annual SOC 2 report, to validate the operating effectiveness of the GCP backup and recovery controls.

Data Communications

The Mantl infrastructure was architected with data encrypted communication channels between the application and database. All unnecessary communication ports and services have been disabled throughout the infrastructure stack. IP whitelisting is used to only allow traffic from authorized devices and locations.

In addition, Mantl utilizes Tenable to identify development and production environment vulnerabilities on an ongoing basis. Management investigates and resolves medium and high-risk vulnerabilities noted in a timely manner.

Boundaries of the System

The scope of this report includes the Financial Software-as-a-Service Platform Services System performed in the San Francisco, California facility.

This report does not include the Know Your Customer/Anti Money Laundering (KYC/AML) identity verification services provided by Alloy at the New York, New York facility, credit card processing and payment services provided by First Data at the Boston, Massachusetts facility, the banking data Application Programming Interface (API) system services provide by Plaid at the San Francisco, California facility, the transactional and marketing email platform services provided by SendGrid at the Denver, Colorado facility and cloud hosting services provided by GCP at multiple facility.

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

Control Environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Mantl's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Mantl's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

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

- Formally, documented code of conduct communicates entity values and behavioral standards to personnel
- Comprehensive Information Security policies and procedures require employees to sign an acknowledgment form upon hiring and annually to confirm that they understand their responsibility for adhering to the policies and procedures contained within the manual
- Employees are required to sign a Confidentiality Agreement and non-disclosure statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties
- Pre-hire screening of all potential employees includes thorough background investigations

Commitment to Competence

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

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

- Management screens all technical candidates thoroughly to ensure that they possess the requisite skills to fulfill their responsibilities at Mantl
- Annual Security Awareness Training is attended by all personnel which focuses on maintaining the security, availability and confidentiality of the proprietary and customer-servicing systems and related data
- Management supports employee training required to maintain technical proficiency and professional licenses held by employees

- Employees receive periodic reviews by their supervisors inclusive of discussing any deficiencies noted in the execution of the Mantl internal and information security controls

Management's Philosophy and Operating Style

Mantl's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel.

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

- Business and industry risks discussed during the periodic management risk assessment meetings, discussed below, and that impact all employees are communicated to the employee base via conferences or email by management
- Annual Security Awareness Training is attended by all personnel which focuses on maintaining the security, availability and confidentiality of the proprietary and customer-servicing systems and related data
- Mantl's management team has frequent, direct communication via "stand-up" and similar meetings with employees to ensure employees understand the most critical tasks and receive clear guidance from management on those tasks

Organizational Structure and Assignment of Authority and Responsibility

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

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

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

- Organizational charts are in place to communicate key areas of authority and responsibility. These charts are communicated to employees and updated as needed
- Key controls that help ensure the security, availability and confidentiality of the products and services provided to customers are assigned to employee “owners” who are responsible for the timely execution of the controls

In addition to the annual Security Awareness Training, the employee-base would receive notification in the event that Mantl experienced a significant security breach or other incident in accordance with the Incident Response policy and procedures.

Human Resource Policies and Practices

Mantl's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Mantl's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

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

- New employees are required to sign acknowledgement forms for the Confidentiality Agreement and Code of Conduct following new hire orientation upon hire
- Employees receive periodic reviews by their supervisors inclusive of discussing any deficiencies noted in the execution of the Mantl internal and information security controls
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist

Risk Assessment Process

Mantl holds an annual risk assessment that quantifies the impact and probability of each risk, the controls in place that mitigate each risk, and management's plan of action with regards to all residual risks over the next twelve months. Mantl identifies and manages risks that would jeopardize the achievement of strategic objectives and risks to the Information Technology (IT) infrastructure supporting its products, as well as specific fraud risks that could threaten the security, confidentiality, and availability of customer data. Mantl identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

Management holds monthly Risk and Security Team meetings which include key members of the executive team as well as other key individuals to address the IT risks identified and tracked via the automated ticket workflow management system.

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

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

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

Integration with Risk Assessment

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

Information and Communications Systems

Mantl’s management is involved with day-to-day operations and is able to provide personnel with an understanding of their individual roles and responsibilities pertaining to internal controls. This includes the extent to which personnel understand how their activities relate to the work of others and the means of reporting exceptions to a higher level within Mantl. Key controls that help ensure the security, availability and confidentiality of the products and services provided to customers are assigned to employee “owners” who are responsible for the timely execution of the controls.

Management believes that open communication channels help ensure that exceptions are reported and acted on in a timely fashion. To reinforce the importance of timely communication, formal communication tools such as organizational charts, employee handbooks, training classes and annual performance reviews are in place. Management's communication activities are made electronically, verbally, and through the actions of management.

Mantl provides guidance to customers during the onboarding process to educate them on how to securely use Mantl applications and provide data in a secure manner. Mantl has also established procedures for the communication to clients in the event that systems or services will be unavailable for a period of time. Examples would include emails to impacted customers in the event of a disaster or during a scheduled system maintenance window.

Monitoring Controls

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

On-Going Monitoring

As noted throughout the system description, Mantl has deployed a number of system and data monitoring tools that control owners are responsible for monitoring and responding in a timely fashion. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications. Issues noted that require changes to be made to information systems supporting customers or the Mantl infrastructure are tracked via the ticketing system and adhere to the change management procedures and controls through resolution.

Management's close involvement in Mantl'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 the security, availability and confidentiality of the systems and data and to maximize the performance of Mantl's personnel. The monthly Risk and Security Team meetings are a key component of Mantl's monitoring of the monitoring tools, the risk and threat landscape, and the execution of controls by Mantl personnel.

Vendor Management

Mantl has defined the following activities to oversee controls performed by vendors that could impact the Financial SaaS Services System:

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

Reporting Deficiencies

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

Changes to the System Since the Last Review

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

Incidents Since the Last Review

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

Criteria Not Applicable to the System

All Common/Security, Availability, and Confidentiality criteria were applicable to the Fin Technologies, Inc. dba Mantl Financial Software-as-a-Service Platform Services System.

Subservice Organizations

This report does not include the KYC/AML identity verification services provided by Alloy, credit card processing and payment services provided by First Data, cloud hosting services provided by GCP, the banking data API system services provide by Plaid, nor the transactional and marketing email platform services provided by SendGrid.

Subservice Description of Services

Alloy - is the Identity Decisioning Platform that assists banks and fintech companies automate their decisions for onboarding, transaction monitoring and credit underwriting.

First Data - Provides secure and innovative payment technology and services solutions to merchants, including small and mid-sized businesses, financial institutions, and government agencies around the world.

GCP - Cloud services provider for Mantl servers, infrastructure, databases, and other cloud building blocks.

Plaid - Instant Account Verification (IAV) provider allowing end users to easily obtain their bank account and routing numbers by providing their bank account login information. Plaid outsources its physical facility security to Amazon Web Services (AWS). Plaid ensures that AWS has sufficient availability and security control in place and monitors adherence to those processes and procedures.

SendGrid - Customer communication platform for transactional and marketing email. SendGrid outsources its physical facility security to Steadfast data center. SendGrid ensures that Steadfast has sufficient availability and security control in place and monitors adherence to those processes and procedures.

Complementary Subservice Organization Controls

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

The following subservice organization controls should be implemented by Alloy to provide additional assurance that the control objectives described within this report are met:

Subservice Organization - Alloy		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.1	Documented policies and procedures are in place regarding systems authentication and access.
		Documented hardening procedures are in place for setting up and hardening servers.
		Assets are assigned owners who are responsible for evaluating access based on job roles.
		The entity uses a Single Sign On (SSO) functionality to access the entity's network and applications.
		Asymmetric keys are utilized to authenticate to the server.
		A role-based security process has been defined with an access control system that is required to use roles when possible.

The following subservice organization controls should be implemented by First Data to provide additional assurance that the control objectives described within this report are met:

Subservice Organization - First Data		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.1	Electronic files with approved funding transactions from customers are processed accurately and timely to initiate funding of new customer accounts via Automated Clearing House (ACH) or debit card/credit processing.

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

Subservice Organization - GCP		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.4/ CC7.2	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.

Subservice Organization - GCP		
Category	**Criteria**	**Control**
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
Availability	A1.2	Google-owned data centers are protected by fire detection and suppression systems.
		Google-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
		Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Google-owned data centers.
		Google-owned data centers have generators to provide backup power in case of electrical failure.
		Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, UPS units, and redundant power supplies.
		GCP performs periodic reviews of colocation service providers to validate adherence with GCP security and operational standards.
		Google Cloud Storage (GCS)-Specific - Google Cloud Storage performs continuous integrity checks of the data at rest. Objects are continuously validated against their checksums to prevent object corruption.
		GCS-Specific - When disk corruption or device failure is detected, the system automatically attempts to restore normal levels of object storage redundancy.
		GCS-Specific - Objects are stored redundantly across multiple fault-isolated facilities.
		GCS-Specific - The design of systems is sufficiently redundant to sustain the loss of a data center facility without interruption to the service.
		Google Cloud PostgreSQL-Specific - If enabled by the customer, Google Cloud PostgreSQL backs up customer databases, stores backups for user-defined retention periods, and supports point-in-time recovery.
		Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.
		Incidents are logged within a ticketing system, assigned severity rating and tracked to resolution.

Subservice Organization - GCP		
Category	**Criteria**	**Control**
		Critical GCP system components are replicated across multiple Availability Zones and backups are maintained.
		Backups of critical GCP system components are monitored for successful replication across multiple Availability Zones.

The following subservice organization controls should be implemented by Plaid to provide additional assurance that the control objectives described within this report are met:

Subservice Organization - Plaid		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.4	Key Management Services (KMS)-Specific - Recovery key materials used for disaster recovery processes by KMS are physically secured offline so that no single AWS employee can gain access to the key material.
		KMS-Specific - Access attempts to recovery key materials are reviewed by authorized operators on a cadence defined in team processes.
		Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed CCTV. Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
Availability	A1.2	Amazon-owned data centers are protected by fire detection and suppression systems.
		Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
		UPS units provide backup power in the event of an electrical failure in Amazon-owned data centers.
		Amazon-owned data centers have generators to provide backup power in case of electrical failure.
		Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, UPS units, and redundant power supplies.

Subservice Organization - Plaid		
Category	**Criteria**	**Control**
		AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards.
		Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.
		Incidents are logged within a ticketing system, assigned severity rating, and tracked to resolution.
		Critical AWS system components are replicated across multiple Availability Zones and backups are maintained.
		Backups of critical AWS system components are monitored for successful replication across multiple Availability Zones.

The following subservice organization controls should be implemented by SendGrid to provide additional assurance that the control objectives described within this report are met:

Subservice Organization - SendGrid		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.4	Access to physical facilities housing hosted systems is restricted to authorized users.
Availability	A1.2	Environmental mechanisms provide protection over fire, water, power outages, temperature changes and natural disasters.
		Software and recovery infrastructure are implemented over hosted systems.

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

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

COMPLEMENTARY USER ENTITY CONTROLS

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

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

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

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

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

Availability
Availability refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Confidentiality
Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel. Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

Control Activities Specified by the Service Organization

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

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

SECTION 4

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

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

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

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

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

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

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

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Core values are communicated from executive management to personnel through policies, directives, guidelines, the code of conduct and the employee handbook.	Inspected the employee handbook, code of conduct, information security policies and procedures and the company intranet to determine that core values were communicated from executive management to personnel through policies, directives, guidelines, the code of conduct and the employee handbook.	No exceptions noted.
		An employee handbook and code of conduct are documented to communicate workforce conduct standards and enforcement procedures.	Inspected the employee handbook and the code of conduct policies and procedures to determine that an employee handbook and code of conduct were documented to communicate workforce conduct standards and enforcement procedures.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.	Inspected the hiring and termination policies and procedures to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
			Inspected the signed employee handbook and code of conduct acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Prior to employment, personnel are required to complete a background check.	Inspected the completed background check for a sample of new hires to determine that prior to employment, personnel were required to complete a background check.	No exceptions noted.
		Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis.	Inspected the signed employee handbook and code of conduct acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook and code of conduct on an annual basis.	No exceptions noted.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the completed performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
		Sanction policies, which include probation, suspension, and termination, are in place for employee misconduct.	Inspected the employee handbook to determine that sanction policies, which include probation, suspension, and termination, were in place for employee misconduct.	No exceptions noted.
		Employees are directed on how to report unethical behavior in a confidential manner.	Inspected the employee handbook to determine that employees were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Executive management roles and responsibilities are documented and reviewed annually.	Inspected the job description for a sample of executive management job roles and revision history to determine that executive management roles and responsibilities were documented and reviewed annually.	No exceptions noted.
		Executive management defines and documents the skills and expertise needed among its members.	Inspected the job description for a sample of executive management job roles to determine that executive management defined and documented the skills and expertise needed among its members.	No exceptions noted.
		Executive management maintains independence from those that operate the key controls within the environment.	Inspected the organizational chart and the internal controls matrix to determine that executive management maintained independence from those that operate the key controls within the environment.	No exceptions noted.
		Operational management assigns responsibility for and monitors the effectiveness and performance of internal controls implemented within the environment.	Inspected the internal controls matrix and the executive annual review meeting agenda and minutes to determine that operational management assigned responsibility for and monitored the effectiveness and performance of internal controls within the environment.	No exceptions noted.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The organizational chart is updated dynamically as changes are made in the organization.	Inquired of the Security Manager regarding organizational charts to determine that the organizational chart was updated dynamically as changes were made in the organization.	No exceptions noted.
			Inspected the organizational chart to determine that the organizational chart was updated dynamically as changes were made in the organization.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions within the HR software and approved by management prior to posting.	Inspected the job description for a sample of job roles and the company intranet to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the Company intranet.	No exceptions noted.
		Executive management job descriptions are reviewed annually, and updates are made, if necessary.	Inspected the job description for a sample of job roles and the revision history to determine that executive management reviewed job descriptions annually and made updates, if necessary.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.	Inspected the hiring and termination policies and procedures to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the signed employee handbook and code of conduct acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
		Executive management has established proper segregations of duties for key job functions and roles within the organization.	Inspected the organizational chart, the internal controls matrix, and the job description for a sample of job roles to determine that executive management established proper segregations of duties for key job functions and roles within the organization.	No exceptions noted.
		Roles and responsibilities defined in written job descriptions consider and address specific requirements relevant to the system.	Inspected the job description for a sample of job roles to determine that roles and responsibilities defined in written job descriptions considered and addressed specific requirements relevant to the system.	No exceptions noted.
		A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third-parties.	Inspected the third-party security management policies and procedures and the completed vendor risk assessment for a sample of third-parties to determine that a vendor risk assessment was performed on an annual basis which included reviewing the activities performed by third-parties.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.	Inspected the employee handbook and the information security policies and procedures to determine that policies and procedures were in place that outlined the performance evaluation process as well as the competency and training requirements for personnel.	No exceptions noted.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the completed performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
		The entity evaluates the competencies and experience of candidates prior to hiring.	Inspected the interview notes for a sample of new hires to determine that the entity evaluated the competencies and experience of candidates prior to hiring.	No exceptions noted.
		Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring process.	Inspected the job description for a sample of job roles and interview notes for a sample of new hires to determine that job requirements were documented in the job descriptions and candidates' abilities to meet these requirements were evaluated as part of the hiring process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Employees are required to attend continued training annually that relates to their job role and responsibilities.	Inspected the completed training acknowledgement form for a sample of current employees to determine that employees were required to attend continued training annually that relates to their job role and responsibilities.	No exceptions noted.
		Executive management has created a training program for its employees.	Inspected the personnel security management policies and procedures to determine that executive management created a training program for its employees.	No exceptions noted.
		Prior to employment, personnel are required to complete a background check.	Inspected the completed background check for a sample of new hires to determine that prior to employment, personnel were required to complete a background check.	No exceptions noted.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the company intranet.	Inspected the job description for a sample of job roles and the company intranet to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the company intranet.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.	Inspected the hiring and termination policies and procedures to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
			Inspected the signed employee handbook and code of conduct acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
		Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis.	Inspected the signed employee handbook and code of conduct acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook and code of conduct on an annual basis.	No exceptions noted.
		Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.	Inspected the employee handbook and the information security policies and procedures to determine that policies and procedures were in place that outlined the performance evaluation process as well as the competency and training requirements for personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the completed performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
		Executive management reviews the job requirements and responsibilities documented within job descriptions as needed and makes updates, if necessary.	Inspected the job description for a sample of job roles and the revision history to determine that executive management reviewed the job requirements and responsibilities documented within job descriptions as needed and made updates, if necessary.	No exceptions noted.
		Sanction policies, which include probation, suspension, and termination, are in place for employee misconduct.	Inspected the employee handbook to determine that sanction policies, which include probation, suspension, and termination, were in place for employee misconduct.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the company intranet.	Inspected the information security policies and procedures, job description for a sample of job roles and the company intranet to determine that organizational and information security policies and procedures were documented for supporting the functioning of controls and processes and made available to its personnel through the company intranet.	No exceptions noted.
		Edit checks are in place to prevent incomplete or incorrect data from being entered into the system.	Inspected the edit check configurations to determine that edits checks were in place to prevent incomplete or incorrect data from being entered into the system.	No exceptions noted.
		Data flow diagrams are maintained by management to identify the relevant internal and external information sources of the system.	Inspected the data flow diagrams to determine that data flow diagrams were maintained by management to identify the relevant internal and external information sources of the system.	No exceptions noted.
		Data that entered into the system, processed by the system and output from the system is protected from unauthorized access.	Inspected the intrusion detection system (IDS) and encryption configurations to determine that data that was entered into the system, processed by the system, and output from the system was protected from unauthorized access.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Roles and responsibilities are defined in written job descriptions and communicated to personnel through the company intranet.	Inspected the job description for a sample of job roles and the company intranet to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the company intranet.	No exceptions noted.
		The entity's policies and procedures, code of conduct and employee handbook are made available to employees through the company intranet.	Inspected the company intranet to determine that the entity's policies and procedures, code of conduct and employee handbook were made available to employees through the company intranet.	No exceptions noted.
		Upon hire, employees are required to complete information security and awareness training.	Inspected the completed information security and awareness training form for a sample of new hires to determine that upon hire, employees were required to complete information security and awareness training.	No exceptions noted.
		Current employees are required to complete information security and awareness training on an annual basis.	Inspected the completed information security and awareness training form for a sample of current employees to determine that current employees were required to complete information security and awareness training on an annual basis.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.	Inspected the hiring and termination policies and procedures to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the signed employee handbook and code of conduct acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
		Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis.	Inspected the signed employee handbook and code of conduct acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook and code of conduct on an annual basis.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.	Inspected the hiring and termination policies and procedures to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
			Inspected the signed employee handbook and code of conduct acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
		Employees are directed on how to report unethical behavior in a confidential manner.	Inspected the employee handbook to determine that employees were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity's third-party agreement outlines and communicates the terms, conditions, and responsibilities of third-parties.	Inspected the executed third-party agreement for a sample of third-parties to determine that the entity's third-party agreement outlined and communicated the terms, conditions, and responsibilities of third-parties.	No exceptions noted.
		Customer commitments, requirements and responsibilities are outlined and communicated through service agreements.	Inspected the executed customer agreement for a sample of customers to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.	No exceptions noted.
		Changes to commitments, requirements and responsibilities are communicated to third-parties, external users, and customers via updated agreements and website notices.	Inspected the executed customer agreement for a sample of customers and the executed third-party agreement for a sample of third-parties to determine that changes to commitments, requirements and responsibilities were communicated to third-parties, external users and customers via updated agreements and website notices.	No exceptions noted.
		The entity communicates to external parties, vendors, and service providers the system commitments and requirements relating to confidentiality through the use of third-party agreements.	Inspected the executed customer agreement for a sample of customers and the executed third-party agreement for a sample of third-parties to determine that the entity communicated to external parties, vendors, and service providers the system commitments and requirements relating to confidentiality through the use of third-party agreements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Changes to commitments and requirements relating to confidentiality are communicated to third-parties, external users, and customers via updated agreements and website notices.	Inspected the executed customer agreement for a sample of customers and the executed third-party agreement for a sample of third-parties to determine that changes to commitments, requirements and responsibilities were communicated to third-parties, external users and customers via updated agreements and website notices.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Executive management has established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	Inspected the executive annual review meeting agenda and minutes and the internal controls matrix to determine that executive management established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	No exceptions noted.
		Responsible parties are defined and assigned to coordinate and monitor compliance and audit activities.	Inspected the organizational chart, and a sample of job descriptions to determine that responsible parties were defined and assigned to coordinate and monitor compliance and audit activities.	No exceptions noted.
		Key performance indicators of both the business performance and employee performance are developed in alignment with entity objectives and strategies.	Inspected the employee handbook, the information security policies and procedures, the entity's documented objectives and strategies, the executive annual review meeting agenda and minutes, and the completed performance evaluation form for a sample of current employees to determine that key performance indicators of both the business performance and employee performance were developed in alignment with entity objectives and strategies.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Business plans and budgets align with the entity's strategies and objectives.	Inspected the entity's business plans, budget, and documented objectives and strategies to determine that business plans and budgets aligned with the entity's strategies and objectives.	No exceptions noted.
		Entity strategies, objectives and budgets are assessed on an annual basis.	Inspected the executive annual review meeting agenda and minutes and the budget plan to determine that entity strategies, objectives and budgets were assessed on an annual basis.	No exceptions noted.
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Documented policies and procedures are in place to guide personnel when performing a risk assessment.	Inspected the risk assessment policies and procedures to determine that documented policies and procedures were in place to guide personnel when performing a risk assessment.	No exceptions noted.
		Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating, and addressing risks and defining specified risk tolerances.	Inspected the risk assessment policies and procedures to determine that management defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating, and addressing risks and defining specified risk tolerances.	No exceptions noted.
		A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the risk assessment policies and procedures and the completed risk assessment to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.
		For gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, are assigned to process owners based on roles and responsibilities.	Inspected the risk assessment policies and procedures and the completed risk assessment to determine that for gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, were assigned to process owners based on roles and responsibilities.	No exceptions noted.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	On an annual basis, management identifies and assesses the types of fraud that could impact their business and operations.	Inspected the completed risk assessment to determine that, on an annual basis, management identified and assessed the types of fraud that could impact their business and operations.	No exceptions noted.
		As part of management's assessment of fraud risks, management considers key fraud factors such as incentives, pressures, opportunity for unauthorized access or use of data, and employee morale and attitude.	Inspected the completed risk assessment to determine that as part of management's assessment of fraud risks, management considered key fraud factors such as incentives, pressures, opportunity for unauthorized access or use of data, and employee morale and attitude.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the centralized antivirus software dashboard console, IDS configurations and firewall rule sets for the production environment to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		On an annual basis, management reviews the controls implemented within the environment for operational effectiveness and identifies potential control gaps and weaknesses.	Inspected the executive annual review meeting agenda and minutes and the internal controls matrix to determine that on an annual basis, management reviewed the controls implemented within the environment for operational effectiveness and identified potential control gaps and weaknesses.	No exceptions noted.
		Logical access reviews are performed on at least a monthly basis.	Inquired of the Security Manager regarding logical access reviews to determine that logical access reviews were performed on at least a monthly basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the completed identity-aware proxy (IAP) user access review, network user access review, operating system user access review, database user access review and application user access review for a sample of months to determine that logical access reviews were performed on at least a monthly basis.	No exceptions noted.
		Backup restoration tests are performed on an annual basis, as part of the disaster recovery test.	Inspected the completed disaster recovery test results inclusive of backup restoration testing, to determine that data backup restoration tests were performed on an annual basis, as part of the disaster recovery test.	No exceptions noted.
		Vulnerability scans are performed monthly on the environment to identify control gaps and vulnerabilities.	Inspected the completed vulnerability scan results for a sample of months to determine that vulnerability scans were performed annually on the environment to identify control gaps and vulnerabilities.	No exceptions noted.
		A third-party performs a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	Inspected the completed penetration test results to determine that a third-party performed a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the completed performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
		Management obtains and reviews attestation reports of vendors and third parties to evaluate the effectiveness of controls within the third-party's environment on an annual basis.	Inspected the completed third-party attestation report and the vendor risk assessment for a sample of third-parties to determine that management obtained and reviewed attestation reports of vendors and third-parties to evaluate the effectiveness of controls within the third-party's environment on an annual basis.	No exceptions noted.
		A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Senior management assesses the results of the control and risk assessments performed on the environment, annually.	Inspected the executive annual review meeting agenda and minutes, the internal controls matrix, and the completed risk assessment to determine that senior management assessed the results of the control and risk assessments performed on the environment, annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Vulnerabilities, deviations, and control gaps identified from the internal control matrix and risk assessment are documented, investigated, and addressed.	Inspected the completed risk assessment and internal control matrix to determine that vulnerabilities, deviations, and control gaps identified from the internal control and risk assessment were documented, investigated, and addressed.	No exceptions noted.
		Vulnerabilities, deviations, and control gaps identified from the internal control matrix and risk assessment are addressed by those parties responsible for taking corrective actions.	Inspected the completed risk assessment and internal control matrix to determine that vulnerabilities, deviations, and control gaps identified from the internal control matrix and risk assessment were addressed by those parties responsible for taking corrective actions.	No exceptions noted.
		Management tracks whether vulnerabilities, deviations and control gaps identified as part of the evaluations performed are addressed in a timely manner.	Inspected the incident tracking tool to determine that management tracked whether vulnerabilities, deviations and control gaps identified as part of the evaluations performed were addressed in a timely manner.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	As part of the risk assessment process, controls within the environment are modified and implemented to mitigate identified vulnerabilities, deviations, and control gaps.	Inspected the completed risk assessment to determine that as part of the risk assessment process, controls within the environment were modified and implemented to mitigate identified vulnerabilities, deviations, and control gaps.	No exceptions noted.
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Inspected the organizational chart and the internal controls matrix to determine that performance of the internal controls implemented within the environment were assigned to appropriate process owners and operational personnel based on roles and responsibilities.	No exceptions noted.
		Management has documented the relevant controls in place for each key business or operational process.	Inspected the internal controls matrix to determine that management documented the relevant controls in place for each key business or operational process.	No exceptions noted.
		Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	Inspected the internal controls matrix to determine that management incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	Inspected the risk assessment policies and procedures and the completed risk assessment to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
		Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the business continuity and disaster recovery plans to determine that business continuity and disaster recovery plans were developed and updated on an annual basis.	No exceptions noted.
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed business continuity and disaster recovery test results to determine that the business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Organizational and information security policies and procedures are documented and made available to employees through the Company intranet.	Inspected the information security policies and procedures and the Company intranet to determine that organizational and information security policies and procedures were documented and made available to its personnel through the Company intranet.	No exceptions noted.
		Management has documented the controls implemented around the entity's technology infrastructure.	Inspected the internal controls matrix to determine that management documented the controls implemented around the entity's technology infrastructure.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management has established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.	Inspected the internal controls matrix to determine that management established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.	No exceptions noted.
		The internal controls implemented around the entity's technology infrastructure include, but are not limited to: • Restricting access rights to authorized users • Limiting services to what is required for business operations • Authentication of access • Protecting the entity's assets from external threats	Inspected the internal controls matrix to determine that the internal controls implemented around the entity's technology infrastructure included, but were not limited to: • Restricting access rights to authorized users • Limiting services to what was required for business operations • Authentication of access • Protecting the entity's assets from external threats	No exceptions noted.
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Organizational and information security policies and procedures are documented and made available to employees through the Company intranet.	Inspected the information security policies and procedures and the Company intranet to determine that organizational and information security policies and procedures were documented and made available to its personnel through the Company intranet.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The organizational and information security policies and procedures and guidance to detail the day-to-day activities to be performed by personnel.	Inspected the information security policies and procedures and the employee handbook to determine that the organizational and information security policies and procedures detailed the day-to-day activities to be performed by personnel.	No exceptions noted.
		Management has implemented controls that are built into the organizational and information security policies and procedures.	Inspected the information security policies and procedures and the internal controls matrix to determine that management implemented controls that were built into the organizational and information security policies and procedures.	No exceptions noted.
		Process owners and key management are assigned ownership to each key internal control implemented within the entity's environment.	Inspected the internal controls matrix to determine that process owners and key management were assigned ownership to each key internal control implemented within the entity's environment.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the company intranet.	Inspected the job description for a sample of job roles and the company intranet to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the company intranet.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Inspected the organizational chart and the internal controls matrix to determine that performance of the internal controls implemented within the environment were assigned to appropriate process owners and operational personnel based on roles and responsibilities.	No exceptions noted.
		Effectiveness of the internal controls implemented within the environment are evaluated annually.	Inspected the executive annual review meeting agenda and minutes and the internal controls matrix to determine that effectiveness of the internal controls implemented within the environment were evaluated annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Documented policies and procedures are in place regarding systems authentication, access, and security monitoring.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place for system authentication, access, and security monitoring.	No exceptions noted.
	Network (GCP)			
		Network user access is restricted via role-based security privileges defined within the access control system.	Inspected the network user listing and access rights to determine that network user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Network administrative access is restricted to user accounts accessible by authorized personnel.	Inquired of the Security Manager regarding network administrative access to determine that network administrative access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
			Inspected the network administrator listing and access rights to determine that network administrative access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		Network are configured to enforce the following password requirements: • Minimum password length • Password History	Inspected the network password settings to determine that the network was configured to enforce the following password requirements: • Minimum password length • Password History	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Multi-factor authentication is required to access the network.	Inspected the multi-factor authentication settings to determine that multi-factor authentication was required to access the network.	No exceptions noted.
		Network account lockout settings are in place that include session timeout.	Inspected the network account lockout settings to determine that network account lockout settings were in place that included session timeout.	No exceptions noted.
		Network audit logging settings are in place that include: • Query data • Kubernetes session information • Capture ID	Inspected the network audit logging settings and an example network audit log extract to determine that network audit logging settings were in place that included: • Query data • Kubernetes session information • Capture ID	No exceptions noted.
		Network audit logs are maintained and reviewed as needed.	Inquired of the Security Manager regarding network audit logs to determine that network audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected the network audit log settings and an example network audit log extract to determine that network audit logs were maintained and reviewed as needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Operating System (Google Container Optimized)			
		Operating system user access is restricted via role-based security privileges defined within the access control system.	Inspected the operating system user listing and access rights to determine that operating system user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Operating system administrative access is restricted to user accounts accessible by authorized personnel.	Inquired of the Security Manager regarding operating administrative access to determine that operating system administrative access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
			Inspected the operating system administrator listing and access rights to determine that operating system administrative access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		Operating systems are configured to enforce password requirements that include: • Minimum password length • Password History	Inspected the operating system password settings to determine that operating systems were configured to enforce password requirements that include: • Minimum password length • Password History	No exceptions noted.
		Multi-factor authentication is required to access the operating system.	Inspected the multi-factor authentication settings to determine that multi-factor authentication was required to access the operating system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Operating system account lockout settings are in place that include session timeout.	Inspected the operating system account lockout settings to determine that operating system account lockout settings were in place that included session timeout.	No exceptions noted.
		Operating system audit logging settings are in place that include: • Query data • Kubernetes session information • Capture ID	Inspected the operating system audit logging settings and an example operating system audit log extract to determine that operating system audit logging settings were in place that included: • Query data • Kubernetes session information • Capture ID	No exceptions noted.
		Operating system audit logs are maintained and reviewed as needed.	Inquired of the Security Manager regarding operating system audit logs to determine that operating system audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected the operating system audit log settings and an example operating system audit log extract to determine that operating system audit logs were maintained and reviewed as needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Database (PostgreSQL)			
		Database user access is restricted via role-based security privileges defined within the access control system.	Inspected the database user access listing and access rights to determine that database user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Database administrative access is restricted to user accounts accessible by authorized personnel.	Inquired of the Security Manager regarding database administrative access to determine that database administrative access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
			Inspected the database administrator listing and access rights to determine that database administrative access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		Databases are configured to enforce password requirements that include: • Password Length • Complexity	Inspected the database password settings to determine that databases were configured to enforce password requirements that included: • Password Length • Complexity	No exceptions noted.
		Database account lockout settings are in place that include session timeout.	Inspected the database account lockout settings to determine that database account lockout settings were in place that included session timeout.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Database audit logging settings are in place that include: • Query data • Cloud SQL • Capture ID • Kubernetes session information • System events	Inspected the database audit logging settings and an example database audit log extract to determine that database audit logging settings were in place that included: • Query data • Cloud SQL • Capture ID • Kubernetes session information • System events	No exceptions noted.
		Database audit logs are maintained and reviewed as needed.	Inquired of the Security Manager regarding database audit logs to determine that the database audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected the database audit logging settings and an example database audit log extract to determine that database audit logs were maintained and reviewed as needed.	No exceptions noted.
	Application (MANTL Platform)			
		Application user access is restricted via role-based security privileges defined within the access control system.	Inspected the application user listing and access rights to determine that application user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Application administrative access is restricted to user accounts accessible by authorized personnel.	Inquired of the Security Manager regarding application administrative access to determine that application administrative access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
			Inspected the application administrator listing and access rights to determine that application administrative access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		The application is configured to enforce password requirements that include: • Password length • Complexity	Inspected the application password settings to determine that application was configured to enforce password requirements that include: • Password length • Complexity	No exceptions noted.
		Application account lockout settings are in place that include: • Account lockout threshold • Manual account reset by an administrator	Inspected the application account lockout settings to determine that application account lockout settings were in place that included: • Account lockout threshold • Manual account reset by an administrator	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Multi-factor authentication is required to access the application.	Inspected the multi-factor authentication settings to determine that multi-factor authentication was required to access the application.	No exceptions noted.
		Application audit logging settings are in place that include: • Logon events • Failed authentication attempts • Session timeout • Session termination • Creation of user/role • Deletion of user/role • User password changes • Changes to security roles	Inquired of the Security Manager regarding application audit logs to determine that application audit logging settings were in place that included: • Logon events • Failed authentication attempts • Session timeout • Session termination • Creation of user/role • Deletion of user/role • User password changes • Changes to security roles	No exceptions noted.
			Inspected an example application audit log extract to determine that application audit logging settings were in place that included: • Logon events • Failed authentication attempts • Session timeout • Session termination • Creation of user/role • Deletion of user/role • User password changes • Changes to security roles	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Application audit logs are maintained and reviewed as needed.	Inquired of the Security Manager regarding application audit logs to determine that application audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected an example application audit log extract to determine that application audit logs were maintained and reviewed as needed.	No exceptions noted.
	Remote Access (Identity Aware Proxy)			
		The ability to administer Identity-Aware Proxy (IAP) access is restricted to user accounts accessible by authorized personnel.	Inquired of the Security Manager regarding IAP administrator access to determine that the ability to administer IAP access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
			Inspected the IAP administrator listing and access rights to determine that the ability to administer IAP access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		Server certificate-based authentication is used as part of the Transport Layer Security (TLS) encryption with a trusted certificate authority.	Inspected the encryption configurations and digital certificate to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Logical access reviews are performed on at least a monthly basis.	Inquired of the Security Manager regarding logical access reviews to determine that logical access reviews were performed on at least a monthly basis.	No exceptions noted.
			Inspected the completed IAP user access review, network user access review, operating system user access review, database user access review and application user access review for a sample of months to determine that logical access reviews were performed on at least a monthly basis.	No exceptions noted.
		Backup restoration tests are performed on an annual basis, as part of the disaster recovery test.	Inspected the completed disaster recovery test results inclusive of backup restoration testing, to determine that data backup restoration tests were performed on an annual basis, as part of the disaster recovery test.	No exceptions noted.
		Logical access to systems is granted to an employee as a component of the hiring process.	Inspected the hiring procedures, system user access listings, and the supporting user access request ticket for a sample of new hires to determine that logical access to systems was granted to an employee as a component of the hiring process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Logical access to systems is revoked as a component of the termination process.	Inspected the termination procedures, system user access listings, and the completed user offboarding checklist for a sample of terminated employees to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.
		Part of this Criterion is the responsibility of the subservice organizations. Refer to the Subservice Organizations section above for controls managed by the subservice organizations.	Not applicable.	Not applicable.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Documented policies and procedures are in place regarding systems authentication, access, and security monitoring.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place for system authentication, access, and security monitoring.	No exceptions noted.
		Logical access to systems is granted to an employee as a component of the hiring process.	Inspected the hiring procedures, system user access listings, and the supporting user access request ticket for a sample of new hires to determine that logical access to systems was granted to an employee as a component of the hiring process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Logical access to systems is revoked as a component of the termination process.	Inspected the termination procedures, system user access listings, and the completed user offboarding checklist for a sample of terminated employees to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.
		Logical access reviews are performed on at least a monthly basis.	Inquired of the Security Manager regarding logical access reviews to determine that logical access reviews were performed on at least a monthly basis.	No exceptions noted.
			Inspected the completed IAP user access review, network user access review, operating system user access review, database user access review and application user access review for a sample of months to determine that logical access reviews were performed on at least a monthly basis.	No exceptions noted.
		Backup restoration tests are performed on an annual basis, as part of the disaster recovery test.	Inspected the completed disaster recovery test results inclusive of backup restoration testing, to determine that data backup restoration tests were performed on an annual basis, as part of the disaster recovery test.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Part of this Criterion is the responsibility of the subservice organizations. Refer to the Subservice Organizations section above for controls managed by the subservice organizations.	Not applicable.	Not applicable.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Documented policies and procedures are in place regarding systems authentication, access, and security monitoring.	Inspected the log management and monitoring policy to determine that documented policies and procedures were in place for system authentication, access, and security monitoring.	No exceptions noted.
		Logical access to systems is granted to an employee as a component of the hiring process.	Inspected the hiring procedures, system user access listings, and the supporting user access request ticket for a sample of new hires to determine that logical access to systems was granted to an employee as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked as a component of the termination process.	Inspected the termination procedures, system user access listings, and the completed user offboarding checklist for a sample of terminated employees to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.
		Logical access reviews are performed on at least a monthly basis.	Inquired of the Security Manager regarding logical access reviews to determine that logical access reviews were performed on at least a monthly basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the completed IAP user access review, network user access review, operating system user access review, database user access review and application user access review for a sample of months to determine that logical access reviews were performed on at least a monthly basis.	No exceptions noted.
		Backup restoration tests are performed on an annual basis, as part of the disaster recovery test.	Inspected the completed disaster recovery test results inclusive of backup restoration testing, to determine that data backup restoration tests were performed on an annual basis, as part of the disaster recovery test.	No exceptions noted.
	Network (GCP)			
		Network access reviews are completed by management monthly.	Inspected the completed network access review for a sample of months to determine that network access reviews were completed by management monthly.	No exceptions noted.
		Network user access is restricted via role-based security privileges defined within the access control system.	Inspected the network user listing and access rights to determine that network user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Operating System (Google Optimized Container)			
		Operating system access reviews are completed by management monthly.	Inspected the completed operating system access review for a sample of months to determine that operating system access reviews were completed by management monthly.	No exceptions noted.
		Operating system user access is restricted via role-based security privileges defined within the access control system.	Inspected the operating system user listing and access rights to determine that operating system user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
	Database (PostgreSQL)			
		Database access reviews are completed by management monthly.	Inspected the completed database access review for a sample of months to determine that database access reviews were completed by management monthly.	No exceptions noted.
		Database user access is restricted via role-based security privileges defined within the access control system.	Inspected the database user listing and access rights to determine that database user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
	Application (MANTL Platform)			
		Application access reviews are completed by management monthly.	Inspected the completed application access review for a sample of months to determine that application access reviews were completed by management monthly.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Application user access is restricted via role-based security privileges defined within the access control system.	Inspected the application user listing and access rights to determine that application user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	This criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section for controls managed by the subservice organizations.	Not applicable.	Not applicable
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	Policies and procedures are in place to guide personnel in data, hardware and software disposal and destruction.	Inspected the information disposal and data classification policies and procedures to determine that policies and procedures were in place to guide personnel in data, hardware and software disposal and destruction.	No exceptions noted.
		The entity purges confidential data after it is no longer required to achieve the purpose for which the data was collected and processed.	Inquired of the Security Manager regarding the process for purging confidential data to determine that the entity purges confidential data after it was no longer required to achieve the purpose for which data was collected and processed.	No exceptions noted.
			Inspected the data disposal policies and procedures to determine that the entity purges confidential data after it was no longer required to achieve the purpose for which data was collected and processed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting service ticket for a sample of data disposals to determine that the entity purged confidential data after it no longer required to achieve the purpose for which the data was collected and processed.	Testing of the control activity disclosed there were no requests to dispose of data during the review period.
		Policies and procedures are in place for removal of media storing critical data or software.	Inspected the acceptable use policies and procedures to determine that policies and procedures were in place for removal of media storing critical data or software.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Network address translation (NAT) functionality is utilized to manage internal IP addresses.	Inspected the NAT configurations to determine that NAT functionality was utilized to manage internal IP addresses.	No exceptions noted.
		IAP, hyper-text transfer protocol (HTTPS) over TLS are used for defined points of connectivity.	Inspected the encryption configurations and digital certificates to determine that IAP, HTTPS over TLS were used for defined points of connectivity.	No exceptions noted.
		IAP users are authenticated via multi-factor authentication prior to being granted remote access to the system.	Inspected the authentication policy settings to determine that IAP users were authenticated via multi-factor authentication prior to being granted remote access to the system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The ability to administer IAP access is restricted to user accounts accessible by authorized personnel.	Inquired of the Security Manager regarding IAP administrator access to determine that the ability to administer IAP access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
			Inspected the IAP administrator listing and access rights to determine that the ability to administer IAP access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.	Inspected the encryption configurations and digital certificate to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram and firewall rulesets for the production environment to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram and firewall rulesets for the production environment to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		An intrusion detection system (IDS) is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram and IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS is configured to notify personnel upon intrusion detection.	Inspected the IDS configuration, IDS notification settings, and an example IDS alert notification to determine that the IDS was configured to notify personnel upon intrusion detection.	No exceptions noted.
		Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the centralized antivirus software.	Inspected the antivirus software dashboard console and centralized antivirus configurations to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the centralized antivirus software.	No exceptions noted.
		The antivirus software provider pushes updates to the installed antivirus software as new updates are available.	Inspected the centralized antivirus configurations to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates were available.	No exceptions noted.
		Centralized antivirus software is configured to scan workstations in real time.	Inspected the centralized antivirus configurations to determine that the centralized antivirus software was configured to scan workstations in real time.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Part of this Criterion is the responsibility of the subservice organizations. Refer to the Subservice Organizations section above for controls managed by the subservice organizations.	Not applicable.	Not applicable.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Logical access to stored data is restricted to authorized accounts accessible by authorized personnel.	Inquired of the Security Manager regarding stored data access to determine that logical access to stored data was restricted to authorized accounts accessible by authorized personnel.	No exceptions noted.
			Inspected the database administrator listing and access rights to determine that logical access to stored data was restricted to authorized accounts accessible by authorized personnel.	No exceptions noted.
		The entity secures its environment using a multi-layered defense approach that includes firewalls, an IDS and antivirus software.	Inspected the network diagram, IDS configurations, firewall rulesets for the production environment, and antivirus settings to determine that the entity secured its environment using a multi-layered defense approach that included firewalls, an IDS, and antivirus software.	No exceptions noted.
		IAP, HTTPS over TLS are used for defined points of connectivity.	Inspected the encryption configurations and digital certificates to determine that IAP, HTTPS over TLS were used for defined points of connectivity.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.	Inspected the encryption configurations and digital certificate to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.
		IAP users are authenticated via multi-factor authentication prior to being granted remote access to the system.	Inspected the authentication policy settings to determine that IAP users were authenticated via multi-factor authentication prior to being granted remote access to the system.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram and firewall rulesets for the production environment to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram and firewall rulesets for the production environment to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		NAT functionality is utilized to manage internal IP addresses.	Inspected the NAT configurations to determine that NAT functionality was utilized to manage internal IP addresses.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		An IDS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram and the IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS is configured to notify personnel upon intrusion detection.	Inspected the IDS configuration, IDS notification settings, and an example IDS alert notification to determine that the IDS was configured to notify personnel upon intrusion detection.	No exceptions noted.
		Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the centralized antivirus software.	Inspected the antivirus software dashboard console and centralized antivirus configurations to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the centralized antivirus software.	No exceptions noted.
		The antivirus software provider pushes updates to the installed antivirus software as new updates are available.	Inspected the centralized antivirus configurations to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates were available.	No exceptions noted.
		Centralized antivirus software is configured to scan workstations in real time.	Inspected the centralized antivirus configurations to determine that the centralized antivirus software was configured to scan workstations in real time.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Part of this Criterion is the responsibility of the subservice organizations. Refer to the Subservice Organizations section above for controls managed by the subservice organizations.	Not applicable.	Not applicable.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	An immutable filesystem is in place that scans for vulnerabilities prior to deployment.	Inspected the malicious software management policies and procedures and the filesystem configurations to determine that an immutable filesystem was in place that scanned for vulnerabilities prior to deployment.	No exceptions noted.
		Documented change control policies and procedures are in place to guide personnel in the change management process.	Inspected the infrastructure change management and code change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in the change management process.	No exceptions noted.
		Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the centralized antivirus software.	Inspected the antivirus software dashboard console and centralized antivirus configurations to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the centralized antivirus software.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The antivirus software provider pushes updates to the installed antivirus software as new updates are available.	Inspected the centralized antivirus configurations to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates were available.	No exceptions noted.
		Centralized antivirus software is configured to scan workstations in real time.	Inspected the centralized antivirus configurations to determine that the centralized antivirus software was configured to scan workstations in real time.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Management has defined configuration standards in the information security policies and procedures.	Inspected the information security policies and procedures to determine that management had defined configuration standards in the information security policies and procedures.	No exceptions noted.
		Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the centralized antivirus software dashboard console, IDS configurations and firewall rule sets for the production environment to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations, monitoring notification settings, and an example monitoring alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.
		An IDS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram and IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The IDS is configured to notify personnel upon intrusion detection.	Inspected the IDS configuration, IDS notification settings, and an example IDS alert notification to determine that the IDS was configured to notify personnel upon intrusion detection.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the acceptable use policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram and firewall rulesets for the production environment to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram and firewall rulesets for the production environment to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected the information security and incident management policies and procedures to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A third-party performs a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	Inspected the completed penetration test results to determine that a third-party performed a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	No exceptions noted.
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.	Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected the information security and incident management policies and procedures to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	No exceptions noted.
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations, monitoring notification settings, and an example monitoring alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.
		Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the centralized antivirus software dashboard console, IDS configurations and firewall rule sets for the production environment to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		An IDS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram and IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS is configured to notify personnel upon intrusion detection.	Inspected the IDS configuration, IDS notification settings, and an example IDS alert notification to determine that the IDS was configured to notify personnel upon intrusion detection.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram and firewall rulesets for the production environment to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram and firewall rulesets for the production environment to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the centralized antivirus software.	Inspected the antivirus software dashboard console and centralized antivirus configurations to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the centralized antivirus software.	No exceptions noted.
		The antivirus software provider pushes updates to the installed antivirus software as new updates are available.	Inspected the centralized antivirus configurations to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates were available.	No exceptions noted.
		Centralized antivirus software is configured to scan workstations in real time.	Inspected the centralized antivirus configurations to determine that the centralized antivirus software was configured to scan workstations in real time.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the acceptable use policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident response policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The incident response policies and procedures define the classification of incidents based on its severity.	Inspected the incident response policies and procedures to determine that the incident response policies and procedures defined the classification of incidents based on its severity.	No exceptions noted.
		A ticket tracking application is utilized to track and respond to incidents, resolve events, and open change tickets when necessary.	Inquired of the Security Manager regarding security incidents to determine that a ticket tracking application was utilized to track and respond to incidents, resolve events, and open supporting change tickets when necessary.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that a supporting ticket tracking application was required to be utilized to track and respond to incidents, resolve events, and open change tickets when necessary.	No exceptions noted.
			Inspected the supporting incident supporting ticket for a sample of incidents to determine that a ticket tracking application was utilized to track and respond to incidents, resolve events, and supporting open change tickets when necessary.	Testing of the control activity disclosed that there were no security incidents during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident response policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		A ticket tracking application is utilized to track and respond to incidents, resolve events, and open change tickets when necessary.	Inquired of the Security Manager regarding security incidents to determine that a ticket tracking application was utilized to track and respond to incidents, resolve events, and open supporting change tickets when necessary.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that a ticket tracking application was required to be utilized to track and respond to incidents, resolve events, and open supporting change tickets when necessary.	No exceptions noted.
			Inspected the supporting incident supporting ticket for a sample of incidents to determine that a ticket tracking application was utilized to track and respond to incidents, resolve events, and open supporting change tickets when necessary.	Testing of the control activity disclosed that there were no security incidents during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Documented incident response and escalation procedures are in place to guide personnel in addressing the threats posed by security incidents.	Inspected the incident response policies and procedures to determine that documented incident response and escalation procedures were in place to guide personnel in addressing the threats posed by security incidents.	No exceptions noted.
		Resolution of incidents are documented within the ticket and communicated to affected users.	Inquired of the Security Manager regarding security incidents to determine that resolution of incidents was documented within the supporting ticket and communicated to affected users.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that resolution of incidents was required to be documented within the supporting ticket and communicated to affected users.	No exceptions noted.
			Inspected the supporting incident supporting ticket for a sample of incidents to determine that resolution of incidents was documented within the supporting ticket and communicated to affected users.	Testing of the control activity disclosed that there were no security incidents during the review period.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Change management requests are opened for incidents that require permanent fixes.	Inspected the change management policies and procedures to determine that change management requests were required to be opened for incidents that required permanent fixes.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity restores system operations for incidents impacting the environment through activities that include, but are not limited to: • Rebuilding system • Updating software • Installing patches • Removing unauthorized access • Changing configurations	Inspected the information security, incident, and change management policies and procedures to determine that the entity restored system operations for incidents impacting the environment through activities that included, but were not limited to: • Rebuilding system • Updating software • Installing patches • Removing unauthorized access • Changing configurations	No exceptions noted.
		Data backup and restore procedures are in place to guide personnel in performing backup activities.	Inspected the backup and recovery policies and procedures to determine that data backup and restore procedures were in place to guide personnel in performing backup activities.	No exceptions noted.
		Logical access reviews are performed on at least a monthly basis.	Inquired of the Security Manager regarding logical access reviews to determine that logical access reviews were performed on at least a monthly basis.	No exceptions noted.
			Inspected the completed IAP user access review, network user access review, operating system user access review, database user access review and application user access review for a sample of months to determine that logical access reviews were performed on at least a monthly basis.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC8.1	The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Documented change control policies and procedures are in place to guide personnel in the change management process.	Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in the change management process.	No exceptions noted.
		The change management process has defined the following roles and assignments: • Authorization of change by CTO or Director of Engineering • Development-environment change by independent developer • Infrastructure Change Manager • Infrastructure Change Owner • Production Environment Testing - static code analysis completed via a scan performed by GitHub and Veracode and a QA tester • Production Environment Change- reviewed by CTO or Director of Engineer	Inspected the infrastructure change management and code change management policies and procedures to determine that the change management process defined the following roles and assignments: • Authorization of change by CTO or Director of Engineering • Development-environment change by independent developer • Infrastructure Change Manager • Infrastructure Change Owner • Production Environment Testing - static code analysis completed via a scan performed by GitHub and Veracode and a QA tester • Production Environment Change- reviewed by CTO or Director of Engineer	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		System changes are communicated to both affected internal and external users.	Inspected the pull requests and supporting change tickets for a sample of application and infrastructure changes to determine that system changes were communicated to both affected internal and external users.	No exceptions noted.
		Access to implement changes in the production environment is restricted to authorized IT personnel.	Inquired of the Security Manager regarding users with access to deploy changes into the production environment to determine that access to implement changes in the production environment was restricted to authorized IT personnel.	No exceptions noted.
			Inspected the list of users with access to deploy changes into the production environment to determine that access to implement changes in the production environment was restricted to authorized IT personnel.	No exceptions noted.
		System changes are authorized and approved by management prior to implementation.	Inspected the pull requests and supporting change tickets for a sample of application changes and infrastructure changes to determine that system changes were authorized and approved by management prior to implementation.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Prior code is held in the source code repository for rollback capability in the event that a system change does not function as designed.	Inspected the code repository branches to determine that prior code was held in the source code repository for rollback capability in the event that a system change did not function as designed.	No exceptions noted.
		Development and test environments are physically and logically separated from the production environment.	Inspected the separate development, QA, and production environments to determine that development and test environments were physically and logically separated from the production environment.	No exceptions noted.
		System change requests are documented and tracked in a ticketing system.	Inspected the pull requests and supporting change tickets for a sample of application and infrastructure changes to determine that system change requests were documented and tracked in a ticketing system.	No exceptions noted.
		System changes are tested prior to implementation. Types of testing performed depend on the nature of the change.	Inspected the pull requests and supporting change tickets for a sample of application and infrastructure changes to determine that system changes were tested prior to implementation and types of testing performed depended on the nature of the change.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency situation.	Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in implementing changes in an emergency situation.	No exceptions noted.
		The entity creates fictious data using package manager that replaces confidential information with fictious information during the change management process.	Inspected a set of fictitious data used during development activities to determine that the entity created fictious data using package manager that replaces confidential information with fictious information during the change management process.	No exceptions noted.

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

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Identified third-party risks are rated using a risk evaluation process and ratings are approved by management.	Inspected the third-party security management policies and procedures and the completed vendor risk assessment for a sample of third-parties to determine that identified third-party risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
		The entity's third-party agreement outlines and communicates: • The scope of services • Roles and responsibilities • Terms of the business relationship • Communication protocols • Compliance requirements • Service levels • Just cause for terminating the relationship	Inspected the executed third-party agreement for a sample of third parties to determine that the entity's third-party agreement outlined and communicated: • The scope of services • Roles and responsibilities • Terms of the business relationship • Communication protocols • Compliance requirements • Service levels • Just cause for terminating the relationship	No exceptions noted.
		Management obtains and reviews attestation reports of vendors and third parties to evaluate the effectiveness of controls within the third-party's environment.	Inspected the completed third-party attestation report and the vendor risk assessment for a sample of third-parties to determine that management obtained and reviewed attestation reports of vendors and third-parties to evaluate the effectiveness of controls within the third-party's environment on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A formal third-party risk assessment is performed on an annual basis to identify threats that could impair system commitments and requirements.	Inspected the completed vendor risk assessment for a sample of third-parties to determine that a formal third-party risk assessment was performed on an annual basis to identify threats that could impair system commitments and requirements.	No exceptions noted.
		Management has assigned responsibility and accountability for the management of risks associated with third-parties to appropriate personnel.	Inspected the organizational chart and Compliance Manager, Audit Manager, and Risk Manager job description to determine that management assigned responsibility and accountability for the management of risks associated with third-parties to appropriate personnel.	No exceptions noted.
		Management has established exception handling procedures for services provided by third parties.	Inspected the third-party security management policies and procedures to determine that management established exception handling procedures for services provided by third-parties.	No exceptions noted.
		The entity has documented procedures for addressing issues identified with third-parties.	Inspected the third-party security management policies and procedures to determine that the entity documented procedures for addressing issues identified with third-parties.	No exceptions noted.
		The entity has documented procedures for terminating third-party relationships.	Inspected the third-party security management policies and procedures to determine that the entity documented procedures for terminating third-party relationships.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY				
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the centralized antivirus software dashboard console, IDS configurations and firewall rule sets for the production environment to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations, monitoring notification settings, and an example monitoring alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.
		Processing capacity is monitored 24x7x365.	Inspected the monitoring tool configurations to determine that processing capacity was monitored 24x7x365.	No exceptions noted.
		Autoscaling is configured to automatically handle the increased traffic and reduce the cost when the need for resources is lower.	Inspected the autoscaling configurations to determine that autoscaling was configured to automatically handle the increased traffic and reduced the cost when the need for resources was lower.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY				
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The change management process is followed when a change is made to a system as a result of capacity constraint.	Inquired of the Security Manager regarding the change management process to determine that the change management process was followed when a change was made to a system as a result of capacity constraint.	No exceptions noted.
			Inspected the change management policies and procedures to determine that the change management process was required to be followed when a change was made to a system as a result of capacity constraint.	No exceptions noted.
			Inspected the supporting change ticket for a sample change made to a system as a result of a capacity constraint/issue to determine that the change management process was followed when a change was made to a system as a result of capacity constraint.	Testing of the control activity disclosed that there were no capacity constraints that required system changes during the review period.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	Data backup and restore procedures are in place to guide personnel in performing backup activities.	Inspected the backup and recovery policies and procedures to determine that data backup and restore procedures were in place to guide personnel in performing backup activities.	No exceptions noted.
		An automated backup system is utilized to perform scheduled backups.	Inspected the backup system configurations to determine that an automated backup system was utilized to perform scheduled backups.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY				
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Backup restoration tests are performed on an annual basis, as part of the disaster recovery test.	Inspected the completed disaster recovery test results inclusive of backup restoration testing, to determine that data backup restoration tests were performed on an annual basis, as part of the disaster recovery test.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section for controls managed by the subservice organization.	Not applicable.	Not applicable.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	A business continuity plan is documented and in place that outlines the range of disaster scenarios and steps the business will take in a disaster to ensure the timely resumption of critical business operations.	Inspected the business continuity and disaster recovery plans to determine that a business continuity plan was documented and in place that outlined the range of disaster scenarios and steps the business would take in a disaster to ensure the timely resumption of critical business operations.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY				
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The business continuity plan is tested on an annual basis and includes: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster	Inspected the completed business continuity and disaster recovery test results to determine that the business continuity plan was tested on an annual basis and included: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster	No exceptions noted.
		Data backup and restore procedures are in place to guide personnel in performing backup activities.	Inspected the backup and recovery policies and procedures to determine that data backup and restore procedures were in place to guide personnel in performing backup activities.	No exceptions noted.
		An automated backup system is utilized to perform scheduled backups.	Inspected the backup system configurations to determine that an automated backup system was utilized to perform scheduled backups.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE CONFIDENTIALITY CATEGORY				
C1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Documented confidential policies and procedures are in place to meet the entity's objectives related to confidentiality.	Inspected the confidentiality policies and procedures to determine that documented confidential policies and procedures were in place to meet the entity's objectives related to confidentiality.	No exceptions noted.
		An inventory log is maintained of assets with confidential data.	Inspected the inventory of company assets to determine that an inventory log was maintained of assets with confidential data.	No exceptions noted.
		Confidential information is maintained in locations restricted to those authorized to access.	Inquired of the Security Manager regarding access to confidential information to determine that confidential information was maintained in locations restricted to those authorized to access.	No exceptions noted.
			Inspected the database administrator listing and access rights to determine that confidential information was maintained in locations restricted to those authorized to access.	No exceptions noted.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	Documented policies and procedures are in place to guide personnel in data, hardware, and software disposal and destruction.	Inspected the data disposal policies and procedures to determine that policies and procedures were in place to guide personnel in data, hardware, and software disposal and destruction.	No exceptions noted.
		An inventory log is maintained of assets with confidential data.	Inspected the inventory log of company assets to determine that an inventory log was maintained of assets with confidential data.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE CONFIDENTIALITY CATEGORY				
C1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity purges confidential data after it is no longer required to achieve the purpose for which the data was collected and processed.	Inquired of the Security Manager regarding the process for purging confidential data to determine that the entity purges confidential data after it was no longer required to achieve the purpose for which data was collected and processed.	No exceptions noted.
			Inspected the data disposal policies and procedures to determine that the entity purges confidential data after it was no longer required to achieve the purpose for which data was collected and processed.	No exceptions noted.
			Inspected the supporting service ticket for a sample of requests to dispose of data, purge a system, or physically destroy a system to determine that the entity purged confidential data after it no longer required to achieve the purpose for which the data was collected and processed.	Testing of the control activity disclosed there were no requests to dispose of data during the review period.