A-LIGN

Celigo, Inc.

Type 2 SOC 2

2022

celigo

REPORT ON CELIGO, INC.'S DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS RELEVANT TO SECURITY AND AVAILABILITY

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 June 30, 2022

Table of Contents

SECTION 1

ASSERTION OF CELIGO, INC. MANAGEMENT

ASSERTION OF CELIGO, INC. MANAGEMENT

August 11, 2022

We have prepared the accompanying description of Celigo, Inc.'s ('Celigo' or 'the Company') CloudExtend Services System titled "Celigo, Inc.'s Description of Its CloudExtend Services System throughout the period April 1, 2022 to June 30, 2022" (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 CloudExtend Services System that may be useful when assessing the risks arising from interactions with Celigo's system, particularly information about system controls that Celigo 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 and Availability (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*).

Celigo uses Amazon Web Services ('AWS') to provide cloud hosting services and MongoDB Atlas ('MongoDB') to provide database backup monitoring 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 Celigo, to achieve Celigo's service commitments and system requirements based on the applicable trust services criteria. The description presents Celigo's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Celigo'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 Celigo, to achieve Celigo's service commitments and system requirements based on the applicable trust services criteria. The description presents Celigo's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Celigo's controls.

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

a. the description presents Celigo's CloudExtend Services System that was designed and implemented throughout the period April 1, 2022 to June 30, 2022, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period April 1, 2022 to June 30, 2022, to provide reasonable assurance that Celigo's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Celigo's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period April 1, 2022 to June 30, 2022, to provide reasonable assurance that Celigo'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 Celigo's controls operated effectively throughout that period.

Asad Siddiqui

Asad Siddiqui
Chief Information Officer
Celigo, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR’S REPORT

To: Celigo, Inc.

Scope

We have examined Celigo’s accompanying description of its CloudExtend Services System titled "Celigo, Inc.’s Description of Its CloudExtend Services System throughout the period April 1, 2022 to June 30, 2022” (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 June 30, 2022, to provide reasonable assurance that Celigo’s service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (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*).

Celigo uses AWS to provide cloud hosting services and MongoDB to provide database backup monitoring services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Celigo, to achieve Celigo’s service commitments and system requirements based on the applicable trust services criteria. The description presents Celigo’s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Celigo’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 Celigo, to achieve Celigo’s service commitments and system requirements based on the applicable trust services criteria. The description presents Celigo’s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Celigo’s controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

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

Service Organization’s Responsibilities

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

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 Celigo's CloudExtend Services System that was designed and implemented throughout the period April 1, 2022 to June 30, 2022, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period April 1, 2022 to June 30, 2022, to provide reasonable assurance that Celigo's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of Celigo's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period April 1, 2022 to June 30, 2022, to provide reasonable assurance that Celigo'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 Celigo'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 Celigo, user entities of Celigo's CloudExtend Services System during some or all of the period April 1, 2022 to June 30, 2022, business partners of Celigo subject to risks arising from interactions with the CloudExtend 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
August 11, 2022

SECTION 3

CELIGO, INC.’S DESCRIPTION OF ITS CLOUDEXTEND SERVICES SYSTEM THROUGHOUT THE PERIOD APRIL 1, 2022 TO JUNE 30, 2022

OVERVIEW OF OPERATIONS

Company Background

Celigo Inc. (Celigo) is a privately held company founded in December 2005 with over 641 employees in 2022. It is headquartered in San Mateo, California with additional offices in Roseville California, and Hyderabad, India. Celigo is an Integration-Platform-as-a-Service (iPaaS) provider with a mission: to enable best-of-breed integration products so that people can always choose best-of-breed applications to run their business. Celigo's main iPaaS product is called integrator.io, which is an Enterprise level Integration platform. A second product line is CloudExtend, which is “integration for individuals”. Celigo customers include companies of all sizes that use multiple cloud apps.

Description of Services Provided

CloudExtend builds applications that enables end users to integrate Google Workspace and Microsoft 365 with NetSuite and Salesforce.

CloudExtend Excel applications enable users to manage their Salesforce and NetSuite data in Excel, including the ability to create new records and modify existing records. Users can also build near real time dashboards and reports by connecting to their Enterprise Resource Planning (ERP) in a familiar Excel environment.

CloudExtend e-mail applications enable organizations to have 360-degree visibility into customer activity by syncing e-mails, calendars, and files to their Customer Relationship Management (CRM).

Principal Service Commitments and System Requirements

Celigo designs its processes and procedures related to CloudExtend to meet its objectives to enhance end-user productivity. Those objectives are based on the service commitments that Celigo makes to user entities, the laws and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Celigo has established for the services. The CloudExtend services are subject to the security and privacy requirements of the EU / UK General Data Protection Regulation (GDPR), and the California Consumer Privacy Act (CCPA), as well as state privacy or security laws and regulations in the jurisdictions in which Celigo or, in some cases, their customer entities operate.

Security commitments to user entities are documented and communicated in Service Subscription Agreements (SSAs) and other customer agreements such as EU / UK GDPR Data Processing Agreements, as well as in the privacy and cookie policy and descriptions of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

CloudExtend is designed to permit system users to access the information they need based on their role in the endpoint system while restricting them from accessing information not needed for their role.

Encryption technologies are used to protect customer data, both at rest and in transit, inside and outside the CloudExtend production environment. CloudExtend User Interface (UI) connections are all Hypertext Transfer Protocol Secure (HTTPS).

Celigo establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Celigo 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 CloudExtend Service.

Components of the System

Infrastructure and Software

Primary infrastructure and software used to provide Celigo's CloudExtend Services System includes the following:

Primary Infrastructure	
Provider	**Purpose**
AWS	Virtual Private Cloud (VPC) / Network, Primary network for cloud storage and processing used for operations, rulesets for incoming and outgoing traffic through the network and use CloudWatch to monitor the network for potential malicious activity. Virtual Hardware for Amazon Elastic Compute Cloud (EC2) Stacks, Web Application Firewall (WAF), Elastic Load Balancing (ELB)'s, AWS Shield, as well as AWS Services: Route 53, Lambda, Simple Queue Service (SQS), and Simple Storage Service (S3), Cognito
MongoDB Atlas	Primary database to store customer Meta and configuration data
Azure Active Directory	Manage Microsoft Applications used to access Microsoft Graph Application Programming Interface (API)
Azure DevOps	Deploy application code
Stripe	Handle credit card transactions (This used by Chargebee)
Chargebee	Manage user subscriptions
Integrator IO	Make API calls to NetSuite and Salesforce
Intercom	Used for supporting customers via chat
Loggly	Monitoring applications
LogRocket	Monitoring applications
Postmark	Send transactional mails to customers
Domain Name System (DNS) Simple	DNS Registrar
Gandi	DNS Registrar
GoDaddy	DNS Registrar

People

Celigo has a well-defined organizational structure that includes the following core groups that support its products and services:

- Executive Management - is responsible for overall strategy, and the CloudExtend General Manager, in conjunction with Engineering and Security management have the responsibility for ensuring enforcement of controls, approving risk assessments, selection and prioritization of risks to mitigate and providing oversight of Celigo's control environment. Management's role is to ensure personnel are appropriately trained, and that systems and processes are in place to meet system uptime, system-wide security, and consistent service execution
- Product Engineering - is responsible for design, development and testing of all software applications being released, including new features and bug fixes. This team is also responsible for ongoing monitoring and troubleshooting of application incidents. The infrastructure group within product engineering is responsible for all operational aspects of the service. The director of engineering role is responsible for designing and overseeing all processes used within product engineering
- Support - is responsible for project implementations and customer support and ensuring all customer-facing activities follow Celigo policies and procedures. Customer service teams are also responsible for communicating any scheduled or unscheduled outages or issues
- Product Management - is responsible for product requirements and roadmap, product documentation, go-to-market strategy, competitive analysis, facilitating interdepartmental communication and training activities
- Security - is responsible for managing Celigo's security and compliance programs supporting the security and compliance of the product and supporting teams' activities

Celigo's management team is responsible for establishing Information Technology (IT) policies, standards, procedures and guidelines covering access, security, privacy, confidentiality and enforcement of procedures across the organization. Celigo ensures that the policies and standards are reviewed annually and are updated as needed to reflect changes in the operating environment.

The current versions of the policies and procedures are posted on the Wiki and are made available to employees for their use and review. The profile and background of the management team is available on Celigo's website.

To drive clarity and transparency in the hiring process, Celigo has prepared detailed job descriptions highlighting the roles, responsibilities and skill requirements posted on their website for current open positions. The recruiting process includes formal, in-depth, employment interviews to ensure that candidates have relevant qualifications to fulfill responsibilities associated with the roles.

Data

Data, as defined for Celigo's CloudExtend platform, includes all electronic data or information submitted by the customer or extracted by CloudExtend on behalf of the customer to Celigo, to be transferred between customer applications.

This information is with Celigo only while it is being transferred between the customer applications, temporarily held during the transaction, and held for a maximum of thirty days to allow for re-tries if there is an error. The information is transmitted to and from endpoints via secure protocols over insecure networks.

Processes, Policies and Procedures

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

Physical Security

Physical security of the CloudExtend production infrastructure is managed by AWS as part of the agreement with them for the use of their services. The AWS SOC 2 Type 2 Report is reviewed at least annually to assure that physical security is managed appropriately. Refer to the "Subservice Organizations" section below for controls managed by AWS.

Logical Access

Access to Celigo's systems and the information contained in them is controlled via role-based access for access to the information necessary to effectively perform job duties.

Neither Celigo employees nor user entities have unlimited access to information beyond that which is needed for the performance of their jobs. Admin access to Celigo's production systems - production instances of the CloudExtend platform and other supporting infrastructure components is restricted to a limited group of six individuals only. Direct access to the AWS production environment is managed using the AWS Identity and Access Management (IAM) access management tools and includes Multi-Factor Authentication (MFA).

Celigo uses LastPass, a cloud-based password / credential management tool, to store the passwords of all production systems and that of other required tools and applications as well. The systems and tools are grouped into folders within LastPass and access to the folder containing the passwords of the production systems is restricted.

Celigo has established a standardized access control process for licensed users (Customers) to access CloudExtend services. Access to the endpoints is controlled by the user's access rights within NetSuite or Salesforce.

Based on Celigo's access management process, admin users are documented and approved by the access controller and access control maintainers. and in order to remove or modify admin user access upon transfer or termination, the HR team provides a completed termination notification to notify the security admin of the termination. The access control maintainers revoke access to production systems based on the same.

Computer Operations - Backups

Customer data requiring backup fall into two categories: information required for managing user subscriptions and metadata relevant to product / feature usage.

Customer Transient data is not backed up as the transient data S3 bucket is not the customer data repository. This is to avoid proliferation of potentially sensitive data in the backup as the source is outside Celigo's control. Customers are responsible for the data and any backups at the end points of the integrations.

Customer connector related data is backed up by MongoDB Atlas for stored data and retained for:

- 2 days for snapshots (every 6 hours)
- 4 weeks for weekly Snapshots
- 12 months for Monthly Snapshots

Computer Operations - Availability

Incident response policies and procedures are in place 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. Incident response procedures are in place to identify and respond to incidents on the network.

Celigo monitors the capacity utilization of the AWS based computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements. Celigo evaluates the need for additional infrastructure capacity in response to growth of existing customers and / or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Server capacity
- Storage for Database, and transient and persistent data
- Network bandwidth

Celigo has implemented a patch management process to ensure production systems are patched in accordance with vendor recommended operating system patches. Celigo system owners review proposed operating system patches to determine whether the patches are applied. Celigo system owners are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Celigo staff validate that all patches have been installed and if applicable that reboots have been completed.

Availability of the CloudExtend production infrastructure is managed by AWS as part of the agreement with them for the use of their services. The AWS SOC 2 Type 2 Report is reviewed at least annually to assure that availability is managed appropriately. Refer to the “Subservice Organizations” section below for controls managed by AWS.

Change Control

Celigo maintains documented change management 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 approvals.

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 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.

Celigo has implemented a patch management process to ensure infrastructure systems are patched in accordance with vendor recommended operating system patches. Engineering reviews proposed operating system patches to determine whether the patches are applied. Celigo Security Management is responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Celigo staff validate that all patches have been installed and if applicable that reboots have been completed.

Data Communications

Network protections are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Protections are in place for Distributed Denial of Service (DDoS) attacks.

Redundancy is built into the system infrastructure to help ensure that there is no single point of failure.

Penetration testing is conducted annually to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology. The third-party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled / disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing, API testing, as well as testing of controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network.

Vulnerability review is performed on a quarterly basis in accordance with Celigo policy. On-demand scans are performed on an as needed basis. Scans are performed against the staging environment which replicates the production environment. Tools requiring installation in the CloudExtend Services System are implemented through the Change Management process.

Authorized employees may access the system from the Internet through the use of AWS IAM and leading credential management technology. Employees are authenticated through the use of two-factor authentication.

Boundaries of the System

The scope of this report includes the CloudExtend Services System performed in the San Mateo, California facilities.

This report does not include the cloud hosting services provided by AWS and database backup monitoring services provided by MongoDB Atlas.

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 Celigo's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Celigo'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 a code of conduct, as well as by example.

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

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

Commitment to Competence

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

Management's Philosophy and Operating Style

Celigo’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:

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

Organizational Structure and Assignment of Authority and Responsibility

Celigo’s organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Celigo’s management believes that establishing a relevant organizational structure includes consideration of key areas of authority and responsibility and appropriate lines of reporting. Celigo has developed an organizational structure suited to its needs. Roles and responsibilities for designing, developing, implementing, operating, monitoring, and maintaining the system are defined within job descriptions, policies, and procedures.

Each department at Celigo is responsible for maintaining documentation and procedures covering important processes. The core groups supporting Celigo’s CloudExtend platform is discussed under the heading “People” in this section of the report.

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

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

Human Resources Policies and Practices

Celigo has formal HR policies that clearly communicate management practices, expectations, and ethical standards. New employees are made aware of their responsibilities and management’s expectations of them at the time of hiring. Employees are provided with an Employee Handbook and a Security Handbook and sign an acknowledgement form to confirm receipt of the same. Employees are also required to sign an Employee Proprietary Information and Inventions Agreement that specifies the confidentiality requirements, as well as the code of conduct. A training process for new hires is in place. This lists out the required training a new employee must undergo before any work is assigned.

Job requirements are documented in the job descriptions and is available on the Wiki. The hiring manager reviews job descriptions before a job position is made available and updates are made as needed.

Candidates are evaluated based on the description of job and skills posted on the Internet and job requisition form. For potential candidates, appropriate background screening is performed prior to employment. Celigo uses a third-party agency to conduct background checks. The background check process includes checks of criminal history and driving records. Prior to initiating the background check, the individual's consent is required.

Based upon the outcome of the completed background check, the appropriate HR representative makes a recommendation to the hiring team.

Employees have annual performance reviews. Those reviews communicate performance feedback. Celigo has also adopted Objective Key Results that are evaluated on a quarterly basis. A formal training plan is established in areas where employees need additional development.

Risk Assessment Process

On an annual basis, Celigo's Security Management performs a risk assessment to analyze the potential risk to assets. For every identified risk, the likelihood and impact are assessed based on an established risk rating methodology. Potential risk mitigation strategies, contingency plans and triggers for the same are also developed and documented. The risk assessment results are reviewed by management, and management responses and approval of the risk assessment made.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Celigo's CloudExtend services system; as well as the nature of the components of the system result in risks that the criteria will not be met. Celigo 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, Celigo'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

The information systems relevant to the scope of this report are described in the "Software" section of this report. Celigo employees use all tools and applications that are cloud-based and can be accessed through the Internet to perform daily tasks.

The processes for supporting the operation of the CloudExtend platform is documented and posted on the respective department's Wiki page and available to all team members.

Information, regarding how to report security and confidentiality failures, incidents, concerns, and other complaints, is documented within the Security Handbook and published on Celigo's Wiki.

Monitoring Controls

The management and supervisory personnel of Celigo monitor the performance and quality of control operations as a normal part of their activities. The engineering management team and security officers jointly perform an annual assessment of the controls identified in the risk assessment process. This group also perform Quarterly reviews of system access, as well as system vulnerability scans, and other activities to monitor system security.

On-Going Monitoring

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

Reporting Deficiencies

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

Changes to the System Since the Last Review

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

Incidents Since the Last Review

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

Criteria Not Applicable to the System

All Common/Security and Availability criteria were applicable to the Celigo CloudExtend Services System.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS and database backup monitoring services provided by MongoDB Atlas.

Subservice Description of Services

AWS provides core virtual hardware that Celigo configures to provide the services. This includes EC2 servers, Elastic load balancers, AWS WAF, AWS Lambda, Amazon SQS, S3 Buckets, Simple Notification Services (SNS), DynamoDB, API Gateway, CloudWatch, Alarm, CloudFront, AWS System Manager (Parameters), AWS Elastic Container Service (ECS), OpsWorks, CloudFormation, CodePipeline, and CloudTrail. Included in the services are physical security, environmental controls, and power redundancy and backup.

MongoDB Atlas is a Software as a Service (SaaS) DB service used to house the data of customers integration environments, and also live in AWS with the same included services for physical security, environmental controls, and power redundancy and backup.

Complementary Subservice Organization Controls

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

The following subservice organization controls should be implemented by AWS and MongoDB Atlas to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - Amazon Web Services		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4	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.
		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 circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Electronic intrusion detection systems (IDS) are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
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.
		Uninterruptible Power Supply (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, Uninterruptible Power Supply (UPS) units, and redundant power supplies.
		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.

Subservice Organization - Amazon Web Services		
Category	**Criteria**	**Control**
		AWS provides customers the ability to delete their content. Once successfully removed the data is rendered unreadable.
		AWS system components are replicated across multiple Availability Zones and backups are maintained.

Subservice Organization - MongoDB Atlas		
Category	**Criteria**	**Control**
Availability	A1.2	The backup system is configured to automatically replicate backup data to a geographically separate location on a continuous basis.
		Cloud services personnel perform restoration of backup files as a component of business operations on at least an annual basis.

Celigo 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, Celigo performs monitoring of the subservice organization controls, including the following procedures:

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

COMPLEMENTARY USER ENTITY CONTROLS

Celigo's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria requirements related to Celigo's services to be solely achieved by Celigo control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Celigo'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 Celigo.
2. User entities should maintain formal policies that provide guidance for information security and data classification within the organization and the supporting IT environment.
3. User entities are responsible for the establishment and termination of end user licenses for CloudExtend products.
4. User entities are responsible for keeping their user account credentials secure for the Endpoints connected to.
5. User entities are responsible for ensuring the supervision, management, and control of the use of Celigo services by their personnel.
6. User entities are responsible for reviewing notifications from Celigo about changes to CloudExtend.

7. User entities are responsible for any resources created with CloudExtend.
8. User entities are responsible for backing up data on their desktop and within their SaaS endpoints CloudExtend is connecting to.
9. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Celigo services.
10. User entities are responsible for notifying Celigo at cloudextend-security@celigo.com if they detect or suspect a security incident related to CloudExtend.

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

Common Criteria (to the Security and Availability 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.

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 Celigo’s description of the system. Any applicable trust services criteria that are not addressed by control activities at Celigo are described within Section 4 and within the “Subservice Organizations” section above.

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

SECTION 4

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

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

A-LIGN ASSURANCE’s examination of the controls of Celigo was limited to the Trust Services Criteria, related criteria and control activities specified by the management of Celigo and did not encompass all aspects of Celigo’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, the code of conduct and the employee handbook.	Inspected the employee handbooks and code of conduct policies and procedures 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 handbooks and 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 and code of conduct.	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.
		Upon hire, personnel are required to sign a non-disclosure agreement.	Inspected the signed proprietary information and invention assignment agreement for a sample of new hires to determine that upon hire, personnel were required to sign a non-disclosure agreement.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Upon hire, personnel are required to complete a background check.	Inquired of the Human Resources Director regarding new hire background checked to determine that upon hire, personnel were required to complete a background check.	No exceptions noted.
			Inspected the background check policy to determine that upon hire, personnel were required to complete a background check.	No exceptions noted.
			Inspected the completed background checks for a sample of new hires to determine that upon hire, personnel were required to complete a background check.	Testing of the control activity disclosed that a background check was not completed timely for one of 25 new hires sampled.
		Performance evaluations are performed for personnel on an annual basis.	Inspected the completed performance evaluation for a sample of current employees to determine that performance 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 policy and procedures, which include probation, suspension and termination, were in place for employee misconduct.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Employees, customers and third parties are directed on how to report unethical behavior in a confidential manner.	Inspected the whistle blower policy and the ethics reporting contact information on the corporate website to determine that employees, customers and third parties were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.
		Executive management roles and responsibilities are documented and reviewed annually.	Inspected the executive management job descriptions including revision dates to determine that executive management roles and responsibilities were documented and reviewed annually.	No exceptions noted.
		Executive management evaluates the skills and expertise of its members annually.	Inspected the performance evaluation form for a sample of executive management members to determine that executive management evaluated the skills and expertise of its members annually.	No exceptions noted.
		Executive management maintains independence from those that operate the key controls within the environment.	Inspected the organizational chart and the completed internal controls matrix to determine that executive management maintained independence from those that operate the key controls within the environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Executive management meets annually with operational management to assess the effectiveness and performance of internal controls within the environment.	Inquired of the Director of Security and Compliance regarding internal controls to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls within the environment.	No exceptions noted.
			Inspected the completed internal controls matrix and the management meeting documentation to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls within the environment.	No exceptions noted.
		Executive management evaluates the skills and competencies of those that operate the internal controls within the environment annually.	Inspected the completed performance evaluation for a sample of current employees to determine that executive management evaluated the skills and competencies of those that operate the internal controls within the environment annually.	No exceptions noted.
		Operational management assigns responsibility for and monitors the effectiveness and performance of internal controls implemented within the environment.	Inspected the completed internal controls matrix to determine that operational management assigned responsibility for and monitored the effectiveness and performance of internal controls within the environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority.	No exceptions noted.
		Executive management reviews the organizational chart annually and makes updates to the organizational structure and lines of reporting, if necessary.	Inspected the revision history of the organizational chart to determine that executive management reviewed the organizational chart annually and made updates to the organizational structure and lines of reporting, if necessary.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and are available to personnel through the entity's Wiki pages.	Inspected the job description for a sample of job roles and the entity's Wiki pages to determine that roles and responsibilities were defined in written job descriptions and were available to personnel through the entity's Wiki pages.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.	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, 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Roles and responsibilities defined in written job descriptions consider and address specific requirements relevant to the system.	Inspected the job descriptions for a sample of job roles to determine that roles and responsibilities defined in written job descriptions considered and addressed specific requirements relevant to the system.	No exceptions noted.
		A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third parties.	Inspected the vendor risk assessment policy and procedure and the completed vendor risk assessment to determine that a vendor risk assessment was performed on an annual basis which included reviewing the activities performed by third parties.	No exceptions noted.
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 performance evaluation documentation and procedures and the employee handbook 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 evaluations are performed for personnel on an annual basis.	Inspected the completed performance evaluation for a sample of current employees to determine that performance evaluations were performed for personnel on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		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.
		The entity has a recruiting department that is responsible for attracting individuals with competencies and experience that align with the entity's goals and objectives.	Inspected the Corporate website and job opening postings to determine that the entity had a recruiting department that was responsible for attracting individuals with competencies and experience that aligned with the entity's goals and objectives.	No exceptions noted.
		Employees are required to attend security awareness training annually.	Inspected the completed information security awareness training for a sample of current employees to determine that employees were required to attend security awareness training annually.	No exceptions noted.
		Executive management has created a training program for its employees.	Inspected the information security and awareness training materials to determine that executive management created a training program for its employees.	No exceptions noted.
		The entity assesses training needs on an annual basis.	Inspected the training assessment questionnaire to determine that the entity assessed the training needs on an annual basis.	No exceptions noted.
		Upon hire, personnel are required to complete a background check.	Inquired of the Human Resources Director regarding new hire background checked to determine that upon hire, personnel were required to complete a background check.	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 background check policy to determine that upon hire, personnel were required to complete a background check.	No exceptions noted.
			Inspected the completed background checks for a sample of new hires to determine that upon hire, personnel were required to complete a background check.	Testing of the control activity disclosed that a background check was not completed timely for one of 25 new hires sampled.
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 are available to personnel through the entity's Wiki pages.	Inspected the job description for a sample of job roles and the entity's Wiki pages to determine that roles and responsibilities were defined in written job descriptions and were available to personnel through the entity's Wiki pages.	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 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 which requires adherence to the personnel's job role and responsibilities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.	Inspected the employee performance evaluation documentation and procedures and the employee handbook 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 evaluation 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 included probation, suspension and termination were in place for employee misconduct.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's Wiki pages.	Inspected the information security policies and procedures and the entity's Wiki pages 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 entity's Wiki pages.	No exceptions noted.
		Data flow diagrams are documented and maintained by management to identify the relevant internal and external information sources of the system.	Observed the data flow diagram to determine that data flow diagrams were documented and maintained by management to identify the relevant internal and external information sources of the system.	No exceptions noted.
		Data that entered into the system, processed by the system and output from the system is protected from unauthorized access.	Inspected the IDS configurations and encryption configurations to determine that data entered into the system, processed by the system and output from the system was protected from unauthorized access.	No exceptions noted.
		Data and information critical to the system is assessed annually for relevance and use.	Inspected the privacy and security risk analysis to determine that data and information critical to the system was assessed annually for relevance and use.	No exceptions noted.
		Data is only retained for as long as required to perform the required system functionality, service or use.	Inspected the document management and retention policy to determine that data was only retained for as long as required to perform the required system functionality, service or use.	No exceptions noted.

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 are available to personnel through the entity's Wiki pages.	Inspected the job description for a sample of job roles and the entity's Wiki pages to determine that roles and responsibilities were defined in written job descriptions and were available to personnel through the entity's Wiki pages.	No exceptions noted.
		The entity's policies and procedures, code of conduct and employee handbook are made available to employees through the entity's Wiki pages.	Inspected the entity's Wiki pages to determine that the entity's policies and procedures, code of conduct and employee handbook were made available to personnel through the entity's Wiki pages.	No exceptions noted.
		Upon hire, employees are required to read and acknowledge the information security policies and procedures and complete information security and awareness training.	Inspected the information security and awareness training tracking tool for a sample of new hires to determine that upon hire, employees were required to read and acknowledge the information security policies and procedures and 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 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.	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.
		Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel’s job role and responsibilities.	Inspected the signed employee handbook for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.	No exceptions noted.
		Executive management meets annually with operational management to discuss the entity’s objectives as well as roles and responsibilities.	Inspected the management meeting minutes to determine that executive management met annually with operational management to discuss the entity's objectives as well as roles and responsibilities.	No exceptions noted.
		Employees, customers and third parties are directed on how to report unethical behavior in a confidential manner.	Inspected the whistle blower policy and the ethics reporting contact information on the corporate website to determine that employees, customers and third parties were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.
		Changes to job roles and responsibilities are communicated to personnel through e-mail communication.	Inspected the entity's e-mail communication to determine that changes to job roles and responsibilities were communicated to personnel through e-mail communication.	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 personnel through the entity's Wiki pages.	Inspected the incident management and the incident response policies and procedures 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 Wiki pages.	No exceptions noted.
		The entity's objectives, including changes made to the objectives, are communicated to its personnel through the entity's Wiki pages.	Inspected the entity's Wiki pages to determine that the entity's objectives, including changes made to the objectives, were communicated to its personnel through the entity's Wiki pages.	No exceptions noted.
		Employees are required to attend security awareness training annually.	Inspected the completed information security awareness training for a sample of current employees to determine that employees were required to attend security awareness training annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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 • Communicates the system commitments and requirements of third parties, including those relating to confidentiality • Communicates the terms, conditions, and responsibilities of third parties	Inspected the customer master agreement templates and the customer agreements for a sample of customers to determine that the entity's third-party agreement: • Delineates the boundaries of the system and describes relevant system components • Communicates the system commitments and requirements of third parties, including those relating to confidentiality • Communicates the terms, conditions, and responsibilities of third parties	No exceptions noted.
		The information security policies and procedures that communicate the system commitments and requirements of external users are provided to external users prior to allowing them access to the system.	Inspected the entity's third-party agreement template and customer contract template to determine that the information security policies and procedures that communicate the system commitments and requirements of external users were provided to external users prior to allowing them access to the system.	No exceptions noted.
		Customer commitments, requirements and responsibilities are outlined and communicated through service agreements.	Inspected the customer master agreement templates and the customer agreements for a sample of customers to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Changes to commitments, requirements and responsibilities are communicated to third parties, external users, and customers via e-mail.	Inspected the entity's newsletters to determine that changes to commitments, requirements and responsibilities were communicated to third parties, external users and customers via e-mail.	No exceptions noted.
		Employees, customers and third parties are directed on how to report unethical behavior in a confidential manner.	Inspected the whistle blower policy and the ethics reporting contact information on the corporate website to determine that employees, customers and third parties were directed on how to report unethical behavior in a confidential manner.	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 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 analysis policy and standard 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 has established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	Inspected the documented key performance indicators 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 compliance job descriptions to determine that responsible parties were defined and assigned to coordinate and monitor compliance and audit activities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Key performance indicators of both the business performance and employee performance are developed in alignment with entity objectives and strategies.	Inspected the employee performance evaluation documentation and procedures, the entity's documented objectives and strategies, and the documented key performance indicators to determine that key performance indicators of both the business performance and employee performance were developed in alignment with entity objectives and strategies.	No exceptions noted.
		Business plans and budgets align with the entity's strategies and objectives.	Inspected the entity's documented objectives and strategies and budget 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 management meeting minutes 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 analysis policy and standard to determine that documented policies and procedures were in place to guide personnel when performing a risk assessment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks, and defining specified risk tolerances.	Inspected the risk analysis policy and standard 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 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 threats from vendors, environmental threats, and unintentional threats • Assessing the likelihood of identified threats and vulnerabilities • Identifying and assessing the impact of the vulnerabilities associated with the identified threats and vulnerabilities • Making recommendations for remediation of control gaps	Inspected the risk analysis policy and standard and the completed risk assessment to determine that the entity's risk assessment process included: • Identifying threats from vendors, environmental threats, and unintentional threats • Assessing the likelihood of identified threats and vulnerabilities • Identifying and assessing the impact of the vulnerabilities associated with the identified threats and vulnerabilities • Making recommendations for remediation of control gaps	No exceptions noted.
		Identified risks are rated using a risk evaluation process and ratings are approved by management.	Inspected the risk analysis policy and standard 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
		Risks identified as a part of the risk assessment process are addressed using one of the following strategies: • Remediate the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the risk analysis policy and standard and the completed risk assessment to determine that risks identified as a part of the risk assessment process were addressed using one of the following strategies: • Remediate the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the risk analysis policy and standard 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 analysis policy and standard 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.
		The annual comprehensive risk assessment results are reviewed and approved by appropriate levels of management.	Inspected the risk analysis policy and standard and the completed risk assessment to determine that the annual comprehensive risk assessment results were reviewed and approved by appropriate levels of management.	No exceptions noted.

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**
		As part of the annual risk assessment, management reviews the potential threats and vulnerabilities arising from its customers, vendors, and third parties.	Inspected the risk analysis policy and standard and the completed risk assessment to determine that as part of the annual risk assessment, management reviewed the potential threats and vulnerabilities arising from its customers, vendors, and third parties.	No exceptions noted.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	On an annual basis, management identifies and assesses the types of fraud that could impact their business and operations.	Inspected the completed risk assessment to determine that, on an annual basis, management identified and assessed the types of fraud that could impact their business and operations.	No exceptions noted.
		Identified fraud risks are reviewed and addressed using one of the following strategies: • Remediate the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the completed risk assessment to determine that identified fraud risks were reviewed and addressed using one of the following strategies: • Remediate the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
		As part of management's assessment of fraud risks, management considers key fraud factors such as incentives, pressures, opportunity for unauthorized access or use of data, and employee morale and attitude.	Inspected the completed risk assessment to determine that as part of management's assessment of fraud risks, management considered threats and vulnerabilities that arise from the use of IT.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Changes to the business structure and operations are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the risk analysis policy and standard 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 in key management and personnel are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the risk analysis policy and standard and the completed risk assessment to determine that changes in key management and personnel were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
		Changes to the entity's systems, applications, technologies, and tools are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the risk analysis policy and standard 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 system configurations, the IDS configurations, and the firewall rule sets for the production environments to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		Management reviews policies, procedures and other control documents for accuracy and applicability on an annual basis.	Inspected the security of information and systems policy, the incident management and the incident response policy, and the change management policy to determine that management reviewed policies, procedures and other control documents for accuracy and applicability on an annual basis.	No exceptions noted.
		On an annual basis, management reviews the controls implemented within the environment for operational effectiveness and identifies potential control gaps and weaknesses.	Inspected the management meeting minutes to determine that on an annual basis, management reviewed the controls implemented within the environment for operational effectiveness and identified potential control gaps and weaknesses.	No exceptions noted.

<table>
<tr><th colspan="5">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="5">Monitoring Activities</th></tr>
<tr><th>CC4.0</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td></td><td></td><td>Logical access reviews are performed on a quarterly basis.</td><td>Inspected the completed network, operating system, and database user access review for a sample of quarters to determine that logical access reviews, and backup restoration tests were performed on at least an annual basis.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>Vulnerability scans are performed quarterly on the environment to identify control gaps and vulnerabilities.</td><td>Inspected the completed vulnerability scan review for a sample of quarters to determine that vulnerability scans were performed quarterly on the environment to identify control gaps and vulnerabilities.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>Performance evaluations are performed for personnel on an annual basis.</td><td>Inspected the completed performance evaluation for a sample of current employees to determine that performance evaluations were performed for personnel on an annual basis.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>Management obtains and reviews attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third party’s environment.</td><td>Inspected the completed third-party review 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 vendor or third party’s environment.</td><td>No exceptions noted.</td></tr>
</table>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Senior management assesses the results of the compliance, control, and risk assessments performed on the environment.	Inspected the management meeting minutes to determine that senior management assessed the results of the compliance, control and risk assessments performed on the environment.	No exceptions noted.
		Senior management is made aware of high-risk vulnerabilities, deviations, and controls gaps identified as part of the compliance, control, and risk assessments performed.	Inspected the management meeting minutes to determine that senior management was made aware of high-risk vulnerabilities, deviations and controls gaps identified as part of the compliance, control and risk assessments performed.	No exceptions noted.
		Vulnerabilities, deviations, and control gaps identified from the compliance, control, and risk assessments are communicated to those parties responsible for taking corrective actions.	Inquired of the Director of Security and Compliance regarding vulnerabilities, deviations, and control gaps to determine that vulnerabilities, deviations, and control gaps identified from the compliance, control, and risk assessments were communicated to those parties responsible for taking corrective actions.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the internal controls matrix and the completed risk assessment to determine that vulnerabilities, deviations, and control gaps identified from the compliance, control, and risk assessments were communicated to those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the supporting remediation ticket for a sample of vulnerabilities, deviations, and control gaps to determine that vulnerabilities, deviations, and control gaps identified from the compliance, control, and risk assessments were communicated to those parties responsible for taking corrective actions.	Testing of the control activity disclosed that no vulnerabilities, deviations, or control gaps occurred during the review period.
		Management tracks whether vulnerabilities, deviations, and control gaps identified as part of the evaluations performed are addressed in a timely manner.	Inspected the management meeting minutes to determine that management tracked whether vulnerabilities, deviations and control 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.
		Controls within the environment are modified and implemented to mitigate vulnerabilities, deviations, and control gaps identified as part of the various evaluations performed.	Inspected the completed internal controls matrix to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations, and control gaps identified as part of the various evaluations performed.	No exceptions noted.
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Inspected the completed internal controls matrix to determine that performance of the internal controls implemented within the environment were assigned to appropriate process owners and operational personnel based on roles and responsibilities.	No exceptions noted.
		Management has documented the relevant controls in place for each key business or operational process.	Inspected the completed internal controls matrix to determine that management documented the relevant controls in place for each key business or operational process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management has incorporated a variety of controls into their environment that includes manual, automated, preventive, detective, and corrective controls.	Inspected the completed internal controls matrix to determine that management incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	No exceptions noted.
		Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	Inspected the risk analysis policy and standard, the completed risk assessment, and the completed internal controls matrix to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
		Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the business continuity and disaster recovery plan and policy 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Management has documented the relationship and linkage between business processes, the relevant technologies used to support the business processes, and the controls in place to help secure those business processes.	Inspected the completed internal controls matrix to determine that management documented the relationship and linkage between business processes, the relevant technologies used to support the business processes, and the controls in place to help secure those business processes.	No exceptions noted.
		Organizational and information security policies and procedures are documented and made available to personnel through the entity's Wiki pages.	Inspected the information security policies and procedures and the entity's Wiki pages to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's Wiki pages.	No exceptions noted.
		Management has documented the controls implemented around the entity's technology infrastructure.	Inspected the completed internal controls matrix to determine that management documented the controls implemented around the entity's technology infrastructure.	No exceptions noted.
		Management has established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.	Inspected the completed internal controls matrix to determine that management established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		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 completed internal controls matrix to determine that the internal controls implemented around the entity's technology infrastructure included, but were not limited to: - Restricting access rights to authorized users - Limiting services to what is 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 personnel through the entity’s Wiki pages.	Inspected the information security policies and procedures and the entity's Wiki pages to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's Wiki pages.	No exceptions noted.
		The information security policies and procedures detail the day-to-day activities to be performed by personnel.	Inspected the information security policies and procedures to determine that the organizational and information security policies and procedures detailed the day-to-day activities to be performed by personnel.	No exceptions noted.

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 implemented controls that are built into the information security policies and procedures.	Inspected the information security policies and procedures and the completed internal controls matrix to determine that management implemented controls that were built into the organizational and information security policies and procedures.	No exceptions noted.
		Process owners and key management are assigned ownership to each key internal control implemented within the entity’s environment.	Inspected the completed internal controls matrix to determine that process owners and key management were assigned ownership to each key internal control implemented within the entity's environment.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and are available to personnel through the entity’s Wiki pages.	Inspected the job description for a sample of job roles and the entity’s Wiki pages to determine that roles and responsibilities were defined in written job descriptions and were available to personnel through the entity’s Wiki pages.	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 completed internal controls matrix to determine that performance of the internal controls implemented within the environment were assigned to appropriate process owners and operational personnel based on roles and responsibilities.	No exceptions noted.

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

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Network (AWS)			
		Network user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Engineering Manager regarding 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.
			Inspected the network user listing to determine that network user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Network administrative access is restricted to authorized personnel.	Inquired of the Engineering Manager regarding the network administrator listing and access rights to determine that network administrative access was restricted to authorized personnel.	No exceptions noted.
			Inspected the network administrator listing and access rights to determine that network administrative access was restricted to authorized personnel.	No exceptions noted.
		Networks are configured to enforce password requirements that include: • Password history • Password age (minimum & maximum) • Password length • Complexity	Inspected the network password settings to determine that networks were configured to enforce password requirements that included: • Password history • Password age (minimum & maximum) • Password length • Complexity	No exceptions noted.

<table>
<tr><th colspan="5">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="5">Logical and Physical Access Controls</th></tr>
<tr><th>CC6.0</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td></td><td></td><td>Network audit logging configurations are in place that include:
• Account logon events
• Account management
• Logon events
• Policy changes
• System events</td><td>Inspected the network audit logging configurations to determine that network account lockout configurations were in place that included:
• Account logon events
• Account management
• Logon events
• Policy changes
• System events</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>Network audit logs are maintained and reviewed as needed.</td><td>Inquired of the Engineering Manager regarding the network audit logs to determine that network audit logs were maintained and reviewed as needed.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td></td><td>Inspected example network audit log extracts to determine that network audit logs were maintained and reviewed as needed.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td colspan="4"><b>Operating System (AWS Production Instances)</b></td></tr>
<tr><td></td><td></td><td>Operating system user access is restricted via role-based security privileges defined within the access control system.</td><td>Inquired of the Engineering Manager regarding the operating system listing and access rights to determine that operating system user access was restricted via role-based security privileges defined within the access control system.</td><td>No exceptions noted.</td></tr>
</table>

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 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 authorized personnel.	Inquired of the Engineering Manager regarding the operating system administrator 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.
			Inspected the operating system administrator listing and access rights to determine that operating system administrative access was restricted to authorized personnel.	No exceptions noted.
		Operating systems are configured to enforce password requirements that include: • Password history • Password age • Password length • Complexity	Inspected the operating system password settings to determine that operating systems were configured to enforce password requirements that included: • Password history • Password age • Password length • Complexity	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Database (MongoDB)			
		Database user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Engineering Manager regarding 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.
			Inspected the database user listing 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 authorized personnel.	Inquired of the Engineering Manager regarding the database administrator listing and access rights to determine that database administrative access was restricted to authorized personnel.	No exceptions noted.
			Inspected the database administrator listing and access rights to determine that database administrative access was restricted to authorized personnel.	No exceptions noted.
		Database users are authenticated via individually-assigned user accounts and passwords.	Observed a user login to the database to determine that database users were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Database audit logs are maintained and reviewed as needed.	Inquired of the Engineering Manager regarding the database audit logs to determine that database audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected example database audit log extracts to determine that database audit logs were maintained and reviewed as needed.	No exceptions noted.
	Application (CloudExtend)			
		Application user access is restricted via role-based security privileges defined within the access control system.	Inspected the application user listing to determine that application user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Application administrative access is restricted to user accounts accessible by authorized personnel.	Inquired of the Engineering Manager regarding privileged access to determine that application administrative access was restricted to authorized personnel.	No exceptions noted.
			Inspected the application admin listing to determine that application administrative access was restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The application is configured to enforce password requirements that include: • Password length • Complexity	Inspected the application password settings to determine that the application was configured to enforce password requirements that included: • Password length Complexity	No exceptions noted.
		Application users are authenticated via individually-assigned user accounts and passwords.	Observed a user login to the application to determine that application users were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.
		Application audit logs are maintained and reviewed as needed.	Inquired of the Engineering Manager regarding the application audit logs to determine that application audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected example application audit log extracts to determine that application audit logs were maintained and reviewed as needed.	No exceptions noted.
		Server certificate-based authentication is used as part of the Transport Layer Security (TLS) encryption with a trusted certificate authority.	Inspected encryption configurations for data in transit 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 to systems is approved and granted to an employee as a component of the hiring process.	Inquired of the Director of Security and Compliance regarding the user access listings and user access request tickets to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.
			Inspected the hiring procedures, the network, operating system, database, and application user listings and the user access provisioning e-mail communication for a sample of new hires to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked for an employee as a component of the termination process.	Inquired of the Director of Security and Compliance regarding termination procedures to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.
			Inspected the termination procedures, the network, operating system, database, and application user listings and user access revocation e-mail communication 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policies and procedures and the access management policy to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inquired of the Director of Security and Compliance regarding the user access listings and user access request tickets to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.
			Inspected the hiring procedures, the network, operating system, database, and application user listings and the user access provisioning e-mail communication for a sample of new hires to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked for an employee as a component of the termination process.	Inquired of the Director of Security and Compliance regarding termination procedures to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the termination procedures, the network, operating system, database, and application user listings and user access revocation e-mail communication 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 a quarterly basis.	Inspected the completed network, operating system, and database user access review for a sample of quarters to determine that logical access reviews, and backup restoration tests were performed on at least an annual basis.	No exceptions noted.
		Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the Engineering Manager regarding the listings of privileged users to the network, operating system, and database to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
			Inspected the listings of privileged users to the network, operating system, and database to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policies and procedures and the access management policy to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inquired of the Director of Security and Compliance regarding the user access listings and user access request tickets to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.
			Inspected the hiring procedures, the network, operating system, database, and application user listings and the user access provisioning e-mail communication for a sample of new hires to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked for an employee as a component of the termination process.	Inquired of the Director of Security and Compliance regarding termination procedures to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the termination procedures, the network, operating system, database, and application user listings and user access revocation e-mail communication 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.
		Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the Engineering Manager regarding the listings of privileged users to the network, operating system, and database to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
			Inspected the listings of privileged users to the network, operating system, and database to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
		Logical access reviews are performed on a quarterly basis.	Inspected the completed network, operating system, and database user access review for a sample of quarters to determine that logical access reviews, and backup restoration tests were performed on at least an annual 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**
	Network (AWS)			
		Network user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Engineering Manager regarding 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.
			Inspected the network user listing to determine that network user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
	Operating System (AWS Production Instances)			
		Operating system user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Engineering Manager regarding the operating system 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.
			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.

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 (MongoDB)			
		Database user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Engineering Manager regarding 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.
			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 (CloudExtend)			
		Application user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Engineering Manager regarding 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.
			Inspected the application user listing 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 above for controls managed by the subservice organization.	Not applicable.	Not applicable.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity’s objectives.	Policies and procedures are in place to guide personnel in data, hardware, and software disposal and destruction.	Inspected the document management and retention policy to determine that policies and procedures were in place to guide personnel in data, hardware and software disposal and destruction.	No exceptions noted.
		Data that is no longer required for business purposes is rendered unreadable.	Inquired of the Director of Security and Compliance regarding the data disposal process to determine that data that was no longer required for business purposes was rendered unreadable.	No exceptions noted.
			Inspected the document management and retention policies and procedures to determine that data that was no longer required for business purposes was rendered unreadable.	No exceptions noted.
			Inspected the supporting service ticket for a sample of requests to dispose of data to determine that data that was no longer required for business purposes was rendered unreadable.	Testing of the control activity disclosed that no requests to dispose of data occurred during the review period.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.	Inspected encryption configurations for data in transit 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
		Transmission of digital output beyond the boundary of the system is encrypted.	Inspected the encryption configurations for data in transit to determine that transmission of digital output beyond the boundary of the system was encrypted.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram and firewall rule sets for the production environments to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the firewall rule sets for the production environments to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		An IDS is utilized to analyze network events and report possible or actual network security breaches.	Inspected 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 an example IDS audit log extract and alert notification to determine that the IDS is configured to notify personnel upon intrusion detection.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Logical access to stored data is restricted to authorized personnel.	Inquired of the Engineering Manager regarding users with privileged access to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
			Inspected the database user listing and access rights to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
		The ability to access backups is restricted to the authorized DevOps group.	Inquired of the Director of Security and Compliance regarding the ability to access and recall backups to determine that the ability to access backups was restricted to the authorized DevOps group.	No exceptions noted.
			Inspected the list of users with the ability to access backups to determine that the ability to access backups was restricted to the authorized DevOps group.	No exceptions noted.
		Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.	Inspected encryption configurations for data in transit 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**
		A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram and firewall rule sets for the production environments to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the firewall rule sets for the production environments to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		An IDS is utilized to analyze network events and report possible or actual network security breaches.	Inspected 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 an example IDS audit log extract and alert notification to determine that the IDS is configured to notify personnel upon intrusion detection.	No exceptions noted.
		Critical data is stored in encrypted format using Advanced Encryption Standard (AES)-256.	Inspected encryption configurations for data at rest to determine that critical data was stored in encrypted format using AES-256.	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**
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Access to implement changes in the production environment is restricted to authorized IT personnel.	Inquired of the Engineering Manager regarding 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.
			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.
		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 ware in place to guide personnel in the change management process.	No exceptions noted.
		An IDS is utilized to analyze network events and report possible or actual network security breaches.	Inspected 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 an example IDS audit log extract and alert notification to determine that the IDS is configured to notify personnel upon intrusion detection.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs, and unusual system activity.	Inspected the monitoring system configurations, the IDS configurations, and the firewall rule sets for the production environments 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 and an example alert 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 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 an example IDS audit log extract and alert notification to determine that the IDS is 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 rule sets for the production environments to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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.	The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the firewall rule sets for the production environments 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.
		Vulnerability scans are performed quarterly on the environment to identify control gaps and vulnerabilities.	Inspected the completed vulnerability scan review for a sample of quarters to determine that vulnerability scans were performed quarterly on the environment to identify control gaps and vulnerabilities.	No exceptions noted.
		Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident management and the incident response policy to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected the information security and incident management and response 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
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations and an example alert 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 system configurations, the IDS configurations, and the firewall rule sets for the production environments 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.
		An IDS is utilized to analyze network events and report possible or actual network security breaches.	Inspected 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 an example IDS audit log extract and alert notification to determine that the IDS is 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 rule sets for the production environments to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the firewall rule sets for the production environments 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.
	Network (AWS)			
		Network audit logging configurations are in place that include: • Account logon events • Account management • Logon events • Policy changes • System events	Inspected the network audit logging configurations to determine that network account lockout configurations were in place that included: • Account logon events • Account management • Logon events • Policy changes • System events	No exceptions noted.
		Network audit logs are maintained and reviewed as needed.	Inquired of the Engineering Manager regarding the network audit logs to determine that network audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected example network audit log extracts to determine that network audit logs were maintained and reviewed as needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Operating System (AWS Production Instances)			
		Operating system audit logging configurations are in place that include: • Account logon events • Account management • Logon events • Policy changes • System events	Inspected the operating system audit logging configurations and an example operating system audit log extract to determine that operating system audit logging configurations were in place that included: • Account logon events • Account management • Logon events • Policy changes • System events	No exceptions noted.
		Operating system audit logs are maintained and reviewed as needed.	Inquired of the Engineering Manager regarding the operating system audit logs to determine that operating system audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected example operating system audit log extracts to determine that operating system audit logs were maintained and reviewed as needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Database (MongoDB)			
		Database audit logging configurations are in place that include: - Account logon events - Account management - Logon events - Privilege use - System events	Inspected the database audit logging configurations and an example database audit log extract to determine that database audit logging configurations were in place that included: - Account logon events - Account management - Logon events - Privilege use - System events	No exceptions noted.
		Database audit logs are maintained and reviewed as needed.	Inquired of the Engineering Manager regarding the database audit logs to determine that database audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected example database audit log extracts to determine that database audit logs were maintained and reviewed as needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Application (CloudExtend)			
		Application audit logging configurations are in place that include: • Account logon events • Account management • Logon events • Policy changes • System events	Inspected the application audit logging configurations and an example application audit log extract to determine that application audit logging configurations were in place that included: • Account logon events • Account management • Logon events • Policy changes • System events	No exceptions noted.
		Application audit logs are maintained and reviewed as needed.	Inquired of the Engineering Manager regarding the application audit logs to determine that application audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected example application audit log extracts to determine that application audit logs were maintained and reviewed as needed.	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 and the incident 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**
		Resolution of incidents are documented within the ticket and communicated to affected users.	Inquired of the Director of Security and Compliance regarding security incidents to determine that resolution of incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the incident management and 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.
			Inspected the supporting incident ticket for a sample of incidents to determine that the incident response policies and procedures defined the classification of incidents based on its severity.	Testing of the control activity disclosed that no security incidents occurred during the review period.
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inquired of the Director of Security and Compliance regarding security incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected the incident management and response policies and procedures to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the supporting incident ticket for a sample of incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Testing of the control activity disclosed that no security incidents occurred during the review period.
		Identified incidents are analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	Inquired of the Director of Security and Compliance regarding security incidents to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	No exceptions noted.
			Inspected the incident management and response policies and procedures to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting incident ticket for a sample of incidents to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	Testing of the control activity disclosed that no security incidents occurred during the review period.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inquired of the Director of Security and Compliance regarding security incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected the incident management and response policies and procedures to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected an example supporting incident ticket for a sample of incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Testing of the control activity disclosed that no security incidents occurred during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		The actions taken to address identified security incidents are documented and communicated to affected parties.	Inquired of the Director of Security and Compliance regarding security incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected the incident management and response policies and procedures to determine that the actions taken to address identified security incidents were documented and communicated to affected parties.	No exceptions noted.
			Inspected an example supporting incident ticket to determine that the actions taken to address identified security incidents were documented and communicated to affected parties.	Testing of the control activity disclosed that no security incidents occurred during the review period.
		Documented incident response and escalation procedures are in place to guide personnel in addressing the threats posed by security incidents.	Inspected the incident management and 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.

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**
		Critical security incidents that result in a service / business operation disruption are communicated to those affected through tickets.	Inquired of the Director of Security and Compliance regarding incident tracking to determine that critical security incidents that result in a service / business operation disruption were communicated to those affected through ticket.	No exceptions noted.
			Inspected the incident management and response policies and procedures to determine that critical security incidents that result in a service / business operation disruption were communicated to those affected through ticket.	No exceptions noted.
			Inspected an example supporting incident ticket to determine that critical security incidents that result in a service / business operation disruption were communicated to those affected through ticket.	Testing of the control activity disclosed that no security incidents occurred during the review period.
		Identified incidents are analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	Inquired of the Director of Security and Compliance regarding incident tracking to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the incident management and response policies and procedures to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	No exceptions noted.
			Inspected an example supporting incident ticket to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	Testing of the control activity disclosed that no security incidents occurred 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 systems • 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 systems • Updating software • Installing patches • Removing unauthorized access • Changing configurations	No exceptions noted.
		A security incident analysis is performed for critical incidents to determine the root cause, system impact, and to determine the resolution.	Inquired of the Director of Security and Compliance regarding incident tracking to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact, and to determine the resolution.	No exceptions noted.
			Inspected the incident management and response policies and procedures to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact, and to determine the resolution.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the supporting incident ticket for an example critical security incident to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact, and to determine the resolution.	Testing of the control activity disclosed that no critical security incidents occurred during the review period.
		After critical incidents are investigated and addressed, lessons learned are documented and analyzed, and incident response plans and recovery procedures are updated based on the lessons learned.	Inspected the incident management and response policies and procedures to determine that after critical incidents were investigated and addressed, lessons learned were documented and analyzed, and incident response plans and recovery procedures were updated based on the lessons learned.	No exceptions noted.
		A business continuity and disaster recovery plan are documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	Inspected the business continuity and disaster recovery plan and policy 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 disaster recovery plan was tested on an annual 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**
		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 plan and policy 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 ware in place to guide personnel in the change management process.	No exceptions noted.
		The change management process has defined the following roles and assignments: • Authorization of change requests-owner or business unit manager • Development-application design and support department • Testing-quality assurance department • Implementation-software change management group	Inspected the change management policies and procedures to determine that the change management process defined the following roles and assignments: • Authorization of change requests-owner or business unit manager • Development-application design and support department • Testing-quality assurance department • Implementation software change management group	No exceptions noted.
		Access to implement changes in the production environment is restricted to authorized IT personnel.	Inquired of the Engineering Manager regarding 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the 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 supporting change ticket for a sample system changes to determine that system changes were authorized and approved by management prior to implementation.	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 supporting change ticket for a sample of system changes to determine that system change requests were documented and tracked in a ticketing system.	No exceptions noted.
		Previous iterations of the applications are held in a source code repository that can be deployed.	Inspected the source code project repository to determine that previous iterations of the applications were held in a source code repository that could be deployed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		System changes are tested prior to implementation. Types of testing performed depend on the nature of the change.	Observed the testing documentation for a sample of system 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.
			Inspected the supporting change ticket for a sample of system 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.
		Information security policies and procedures document the baseline requirements for configuration of IT systems and tools.	Inspected the information security policies and procedures to determine that information security policies and procedures documented the baseline requirements for configuration of IT systems and tools.	No exceptions noted.
		Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency situation.	Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in implementing changes in an emergency situation.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Documented policies and procedures are in place to guide personnel in performing risk mitigation activities.	Inspected the risk analysis policy and standard 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 analysis policy and standard 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 analysis policy and standard 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**
		Risks identified as a part of the risk assessment process are addressed using one of the following strategies: • Remediate the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the risk analysis policy and standard and the completed risk assessment to determine that risks identified as a part of the risk assessment process were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the risk analysis policy and standard 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.
		The entity has purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	Inspected the insurance documentation to determine that the entity purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Management has defined a third-party vendor risk management process that specifies the process for evaluating third-party risks based on identified threats and the specified tolerances.	Inspected the vendor risk policy and procedure to determine that management defined a third-party vendor risk management process that specified the process for evaluating third-party risks based on identified threats and the specified tolerances.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management obtains and reviews attestation reports of vendors to evaluate the effectiveness of controls within the vendors’ environment.	Inspected the vendor attestation review for a sample of vendors to determine that management obtained and reviewed attestation reports of vendors to evaluate the effectiveness of controls within the vendors’ environment.	No exceptions noted.
		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 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.

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 system configurations, the IDS configurations, and the firewall rule sets for the production environments 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 and an example alert 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.
		Future processing demand is forecasted and compared to scheduled capacity on an annual basis.	Inspected the processing capacity policy and procedure to determine that future processing demand was forecasted and compared to scheduled capacity on an annual basis.	No exceptions noted.
		Future processing demand forecasts are reviewed and approved by management on an annual basis.	Inspected the processing capacity policy and procedure to determine that future processing demand forecasts were reviewed and approved by management on an annual basis.	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**
A1.2	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.	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 plan and policy 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.
		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.

SECTION 5

OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION

MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results	Management's Response
CC1.1, CC1.4	Upon hire, personnel are required to complete a background check.	Inspected the completed background checks for a sample of new hires to determine that upon hire, personnel were required to complete a background check.	Testing of the control activity disclosed that a background check was not completed timely for one of 25 new hires sampled.	**Celigo Management Response:** Celigo management acknowledges the control exception, which revolved around a core issue of follow up for background checks, and an over-reliance on "automated controls" that allowed the background checks to expire several times. For the exception listed, the background check was not completed timely. In regards to (1) listed above, when discovered during Celigo's internal HR audit prior to this SOC 2 audit, Celigo escalated the same issue with the background check vendor - HireRight - and the reason provided for the issue to Celigo was "delayed submissions or lack of submission of the right set of documents by the employee". As soon as the letters of experience were received from the employee in question, Celigo initiated his background check with HireRight. Following this, the employee did not provide his information to the HireRight team within 15 days, and the link expired. The HireRight team did not inform Celigo about this, nor did the employee. The lack of any notification caused the background check to complete late. **Mitigation and Remediation**: Celigo initiated another background check on Feb 2, 2022, and it got completed by Feb 10, 2022. Celigo understood at the time of discovery that the delay needed remedial activity. Celigo has also instituted and maintained tracking of every background check process and made sure they are completed as per the background check policy. At the time of this response, the new procedure is approved and in use, and the HR onboarding staff have been trained in its use.