OneTrust

PRIVACY, SECURITY & GOVERNANCE

OneTrust, LLC

SOC 2 Report

For

Certification Automation

A Type 2 Independent Service Auditor's Report on Controls Relevant to Security, Availability, and Confidentiality

May 1, 2024, to April 30, 2025

Attestation and Compliance Services

schellman

Quality, above all.

This report is intended solely for use by the management of OneTrust, LLC, user entities of OneTrust, LLC’s services, and other parties who have sufficient knowledge and understanding of OneTrust, LLC’s services covered by this report (each referred to herein as a “specified user”).

If the report recipient is not a specified user (herein referred to as a "non-specified user"), use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against Schellman & Company, LLC as a result of such access. Further, Schellman & Company, LLC does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

TABLE OF CONTENTS

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT

Independent Service Auditor's Report

To OneTrust, LLC:

Scope

We have examined OneTrust, LLC's ("OneTrust" or the "service organization") accompanying description of its Certification Automation system, in Section 3, throughout the period May 1, 2024, to April 30, 2025, (the "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 May 1, 2024, to April 30, 2025, to provide reasonable assurance that OneTrust's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).*

OneTrust uses a subservice organization for cloud hosting and managed database services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at OneTrust, to achieve OneTrust's service commitments and system requirements based on the applicable trust services criteria. The description presents OneTrust's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of OneTrust's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

OneTrust 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 OneTrust's service commitments and system requirements were achieved. OneTrust has provided the accompanying assertion, in Section 2, ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. OneTrust 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 (AICPA) and in accordance with International Standard on Assurance Engagements 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board. 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.

Service Auditor's Independence and Quality Control

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement, including the Code of Professional Conduct established by the AICPA and the International Ethics Standards Board for Accountants' Code of Ethics for Professional Accountants.

We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

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 Test of Controls

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

Opinion

In our opinion, in all material respects:

- the description presents OneTrust's Certification Automation system that was designed and implemented throughout the period May 1, 2024, to April 30, 2025, in accordance with the description criteria;
- the controls stated in the description were suitably designed throughout the period May 1, 2024, to April 30, 2025, to provide reasonable assurance that OneTrust's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization applied the complementary controls assumed in the design of OneTrust's controls throughout that period; and

- the controls stated in the description operated effectively throughout the period May 1, 2024, to April 30, 2025, to provide reasonable assurance that OneTrust's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of OneTrust'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 OneTrust, user entities of OneTrust's Certification Automation system during some or all of the period of May 1, 2024, to April 30, 2025, business partners of OneTrust subject to risks arising from interactions with the Certification Automation 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 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; and
- 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.

Schellman & Company, LLC

Tampa, Florida
June 3, 2025

SECTION 2

MANAGEMENT'S ASSERTION

Management's Assertion

We have prepared the accompanying description of OneTrust's Certification Automation system, in Section 3, throughout the period May 1, 2024, to April 30, 2025, (the "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 Certification Automation system that may be useful when assessing the risks arising from interactions with OneTrust's system, particularly information about system controls that OneTrust has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

OneTrust uses a subservice organization for cloud hosting and managed database services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at OneTrust, to achieve OneTrust's service commitments and system requirements based on the applicable trust services criteria. The description presents OneTrust's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of OneTrust's controls. The description does not disclose the actual controls at the subservice organization.

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

- the description presents OneTrust's Certification Automation system that was designed and implemented throughout the period May 1, 2024, to April 30, 2025, in accordance with the description criteria;
- the controls stated in the description were suitably designed throughout the period May 1, 2024, to April 30, 2025, to provide reasonable assurance that OneTrust's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization applied the complementary controls assumed in the design of OneTrust's controls throughout that period; and
- the controls stated in the description operated effectively throughout the period May 1, 2024, to April 30, 2025, to provide reasonable assurance that OneTrust's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of OneTrust's controls operated effectively throughout that period.

SECTION 3

DESCRIPTION OF THE SYSTEM

Overview of Operations

Company Background

OneTrust, LLC ("OneTrust" or "the Company") is Trust Intelligence company, providing solutions that help businesses manage data, ensure compliance, and build trust through responsible data and AI practices, trusted by more than 14,000 customers to comply with the California Consumer Privacy Act (CCPA), General Data Protection Regulation (GDPR), International Organization for Standardization (ISO) 27001 and 27701 standards, and hundreds of the world's privacy and security laws.

Description of Services Provided

OneTrust's Certification Automation system automates information security policy and control creation, risk assessment, compliance management, compliance monitoring, automated and manual evidence collection, security certification gap assessment, audit process management, vendor risk management, and security questionnaire responses so enterprises can gain trust with customers and increase profits. The software creates a scalable governance system of record for business teams to manage security policies and controls that support critical business functions such as information security, user security training, network and system operations, vendor management, and sales, with real-time compliance information needed to complete customer request for proposals (RFPs) and contracts.

The Certification Automation system is a Software as a Service (SaaS) solution that includes a web-based user interface for tracking Information Security program requirements. Customers have the ability to create their own information security program from Certification Automation system's predefined database of policies and controls or upload their own information security program. The solution also enables administrators to upload and respond to security questionnaires automatically utilizing Certification Automation system machine-learning-based Auto-Answer engine. Outputs include an InfoSec policy documents, security assurance reports, completed security questionnaires and vendor security assessments.

Certification Automation system integrates with various platforms to help customers automate their evidence collection. List of integrations available on Certification Automation system:

Related Service	Integrations Offered
Cloud Services	AWS, Google Cloud Platform, Heroku, Digital Ocean, Microsoft Azure
Version Control	Microsoft Azure DevOps, BitBucket, GitHub, GitLab
Workstation Management	Hexnode, JAMF Pro, Jumpcloud, Kandji, Sophos, Microsoft Intune
Employee Population	Bamboo HR, Ceridian Dayforce, Charthop, Freshteam, Google Workplace (GSuite), Gusto, Hibob, HR Cloud, HR Partner, Humaans.io, Justworks, Lano, Microsoft Azure Active Directory, Namely, Nmbrs, Okta, Paychex, Paylocity, Personio, Rippling, Sage HR, SAP SuccessFactors, Sapling, Sesame, Square Payroll, Trinet, UkG Pro, Workday, Zenefits
Other	Certn, Cloudflare, Cobalt, CrowdStrike, Datadog, Jira Cloud, Lacework, OneTrust Consent Management, Slack, Zapier, Zendesk, Knowb4, Shortcut, ServiceNow, Visma Nmbrs

Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of the Certification Automation system. Commitments are communicated in written contracts, the Master Terms of Service, and Service Level Agreements. For the Company's principal service commitments related to the Certification Automation system, OneTrust will:

- Implement appropriate technical and organizational measures to ensure a level of security appropriate to the level of risk and to protect data from accidental or unlawful destruction, loss, alteration, and unauthorized disclosure or access.
- Inform customers without undue delay if OneTrust becomes aware of a security breach and provide reasonable information and cooperation to the customer.
- Make the service available 99.95% of the time in a given calendar month.
- Protect confidential customer information by using the same level of care and discretion it uses with respect to its own confidential information.
- Not use confidential information, except for the purposes of providing the services, or disclose confidential customer information to any person other than its employees or authorized users who have a need to know.
- Promptly destroy customer confidential data upon termination of the services.

System requirements are specifications regarding how the Certification Automation system should function to meet the Company's principal commitments to user entities. System requirements are specified in the Company's policies and procedures.

The Company's system requirements include the following:

- Employee provisioning and deprovisioning standards
- Privileged access reviews
- Logical access standards
- Risk and vulnerability management standards
- System acquisition, development, and maintenance standards
- Change management standards
- Logging and monitoring standards
- Incident handling standards
- Encryption standards
- Vendor management
- Asset management standards

In accordance with OneTrust's assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

Components of the System Used to Provide the Service

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Infrastructure and Software

OneTust utilizes Amazon Web Services, Inc. (AWS) cloud hosting services to provide the resources to host the Certification Automation system. Within various AWS regions, three copies of the system are maintained, two hosted in the United States (U.S.) and one hosted in the European Union (EU). The application stack is composed of a frontend JavaScript application (utilizing React/Redux) and a backend Python API (utilizing Python 3.10). Nginx is utilized as a web server with gunicorn as the Python container.

The Certification Automation system stack in the US is deployed in a VPC in the US-EAST-1 (N. Virginia) region as the primary region with US-WEST-2 (Oregon) as the secondary. The other U.S. region resides in California (CA) known as CA-CENTRAL-1 (Central). This location has no secondary region. The application stack in the EU runs in a Virtual Private Cloud (VPC) in the EU-CENTRAL-1 (Frankfurt) region as the primary region and secondary configured as EU-WEST-1 (Ireland). It currently does not have a secondary region as CA only has one available.

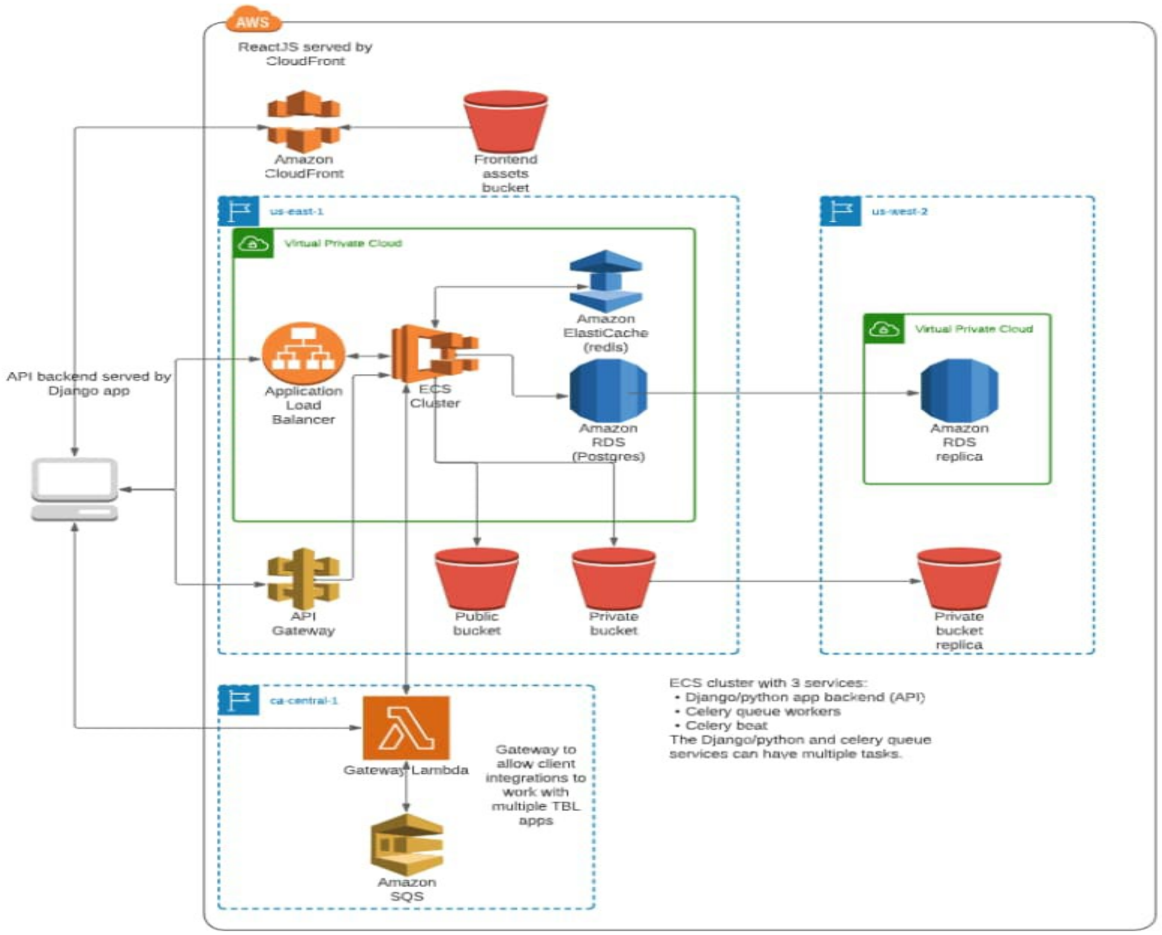
The back-end API application runs in AWS Elastic Container Service (ECS) behind an AWS Elastic Load Bearing (ELB). The front-end JavaScript (JS) application is served from CloudFront, with the assets hosted in Simple Storage Service (S3). All applications utilize AWS ECS for background tasks and utilize AWS API Gateway for the custom API integration feature.

The database supporting the application is utilizing AWS Relational Database Service (RDS) running PostgreSQL 13.4 and is replicated in real-time to the secondary region. AWS ElastiCache (redis) is also utilized. S3 is utilized to store user-uploaded files and is replicated in real-time to the secondary region. CloudWatch is utilized for both monitoring and log storage. Encryption keys are managed through the AWS Key Management Service (KMS). Access to the keys is restricted to a small number of senior team members.

The platform is a SaaS-multi-tenant client server application. Customers receive their own tenant in the Certification Automation system, and their data is encrypted and logically separated and not accessible to other tenants to prevent unauthorized access. Client data locations and data flows are outlined in the diagram below along with the security measures in place to protect this data.

[Intentionally Blank]

The following diagrams identifies the virtual design of the solution, including all places where customer data resides, all data flows and how it is secured by OneTrust:


AWS
ReactJS served by CloudFront
Amazon CloudFront
Frontend assets bucket
us-east-1
Virtual Private Cloud
Amazon ElastiCache (redis)
Application Load Balancer
ECS Cluster
Amazon RDS (Postgres)
API backend served by Django app
API Gateway
Public bucket
Private bucket
us-west-2
Virtual Private Cloud
Amazon RDS replica
Private bucket replica
ca-central-1
Gateway Lambda
Gateway to allow client integrations to work with multiple TBL apps
Amazon SQS
ECS cluster with 3 services:
• Django/python app backend (API)
• Celery queue workers
• Celery beat
The Django/python and celery queue services can have multiple tasks.

The following provides a summary of supporting software systems utilized to deliver the Certification Automation system:

- CloudWatch: utilized for the monitoring of production systems and log storage
- RDS: utilized for the hosting and operation of SQL databases
- ElastiCache: utilized for application performance and scalability
- Route 53: utilized for the management of Domain Name System (DNS) and routing traffic within AWS
- ECS: utilized for container deployment and management
- VPC: utilized for the building of secure, scalable, and customizable architectures within the AWS cloud
- ELB: utilized for the distribution of incoming network traffic across multiple resources
- CloudFront: utilized for the delivery of content to end-users with low latency and high data transfer speeds
- S3: utilized for object storage
- BetterUptime: utilized for system status
- GitHub: utilized for source code version control
- Jira: utilized for tracking development requirements
- ReactJS: utilized for the frontend web application
- Node.js v16: utilized as the gateway server

- Python 3.10: utilized for backend API programming
- SendGrid: utilized for sending application e-mails
- Docker: utilized for the automation of deployments and management of applications in isolated containers
- GitLab: utilized for vulnerability scanning of containers
- Qualys: utilized for vulnerability scanning of applications

People

OneTrust develops, manages, and secures the OneTrust Platform via separate departments. The responsibilities of these departments are defined below.

Information Security and Privacy

Information security and privacy is governed through an Integrated Management System (IMS) Committee ("IMS Committee," "Committee"), which is responsible for working with the IMS chair to ensure the following: (a) that the information security policy and objectives are established; (b) that IMS requirements are identified and integrated into organizational processes in support of the policy and objectives; (c) the availability of the resources that are necessary to ensure the success of the IMS; (d) the communication of IMS policies and procedures and their importance to personnel, as appropriate; (e) that the IMS continuously improves toward achieving its mission; (f) that the IMS has the necessary personnel to achieve its mission; (g) the continual improvement of the IMS through the establishment of objectives; and (h) that department managers are made aware of how they are vital to the success of the IMS.

A team of attorneys focused on privacy and compliance provides development guidance and assists in the identification, implementation, and maintenance of organization-wide information privacy policies and procedures in coordination with organization management, administration, and legal counsel. The privacy team performs initial and periodic privacy impact assessments and conducts related, ongoing compliance monitoring. The team also oversees security and privacy training and orientation for all employees. Finally, the team maintains current knowledge of applicable privacy laws and accreditation standards and monitors advancements in information privacy technologies to ensure organizational adaptation and compliance.

Legal

The primary responsibility of the legal team is to provide transactional support for the OneTrust business. Additionally, the attorneys provide legal advice and counsel to internal clients at all levels on commercial matters, support day-to-day initiatives and long-term strategies of OneTrust, and maintain relationships with external counsel.

Product Management

Product Management defines and drives product requirements, prioritization, and execution pertaining to the development and features of products. The team works with customers and cross-functional team members to define and prioritize market-driven features, functionality, and enhancements. The team drives product planning, development, documentation, customer beta testing, and launch activities.

Professional Services and Support

Professional Services handles the overall responsibility for the customer relationship by working directly with OneTrust customers to enhance their user experience with the services. Members of this team have a clear understanding of the privacy industry, including the regulatory environment, and use this knowledge to support customers. Team members monitor industry trends and customer needs for the purpose of being active and vocal in making decisions about the direction of the services.

Human Resources (HR)

HR drives employee relations and employee engagement activities. In particular, HR prepares for and assists with new-hire onboarding, supports training and development programs, supports performance management and compensation administration, assists employees by listening to concerns and making recommendations for resolutions, assists with benefits programs (including annual open enrolment), and participates in benefits administration.

HR's Recruitment Team supports talent-acquisition activities from inception to completion for all positions. This team manages stakeholder relationships, candidate sourcing, talent selection, interview scheduling, and offer management.

Research and Development (R&D) and Quality Assurance (QA)

R&D applies agile methodologies and problem-solving skills to design, develop, and unit test applications deployed to Azure and assists with cloud application architecture. Additionally, R&D carries out QA audits to ensure that documentation and controls designs are appropriate for the software, then addresses quality issues and follows up and closes pending preventive and corrective action requests. Finally, the Operations roles support OneTrust's infrastructure by using automation to deploy software, configuration changes, and infrastructure changes; to troubleshoot software and infrastructure-as-a-service (IaaS) problems in its cloud environment; and to support application infrastructure to ensure that the software is optimized for performance and reliability.

Procedures

OneTrust maintains and documents operating technology standards and procedures in order to provide staff with centralized up-to-date references and training aids. OneTrust's policies and procedures contain guidance regarding aspects of computer usage and security.

OneTrust has implemented both automated and procedural controls through system tools and through policies and procedures to create the internal control framework. Management's involvement in day-to-day operations allows for real-time review of the operating effectiveness of internal controls.

OneTrust has documented and communicated policies and procedures to its employees to restrict logical access to OneTrust's systems based on the principle of least privilege. These procedures cover the following key security lifecycle areas:

- Policy management and communication
- Selection, documentation, and implementation of security controls
- Authorization, changes to, and termination of information system access
- Password protocol
- Monitoring security controls
- Management of access and roles
- Incident response
- Maintenance of restricted access to system configurations, administrative functionality, passwords, powerful utilities, and security devices

Access, Authentication, and Authorization

OneTrust applies the principle of least privilege and restricts access to the production environment only to those requiring access to perform their job function. Access to the infrastructure within AWS requires initial access to a hardened jump server which requires an Active Directory (AD) account, and the use of multi-factor authentication (MFA). Accounts within AD are unique to specific individuals and sharing of the accounts is prohibited. AD security groups are utilized to ensure functions performed within the production environment are limited based on a user's role within the organization. AD password requirements are also in place to enforce predefined minimum password requirements according to documented policies. Remote sessions to the production environment are configured to automatically terminate after a predefined time period of inactivity. Access to perform administrative functions within the production environment and to the AWS management console is restricted to personnel commensurate with their job role.

Additionally, system components are configured such that the organization and its customers' access is segmented from other tenant users.

Access Requests and Access Revocation

Access to in-scope system components require a documented access request along with manager approval prior to access being provisioned. Termination notifications are provided to relevant teams in the event of an employee termination and system access is revoked as part of the termination process. The identity management system is configured to sync with the HR system to automatically deactivate Entra ID (Azure) user accounts in the event that an employee's employment status is no longer active in the HR system. Quarterly access reviews are performed by management to ensure access to systems within the environment is appropriate.

Change Management

OneTrust maintains and documents change management policies and procedures to guide personnel on application and infrastructure changes to the production environment. A formal system development life cycle (SDLC) methodology is established that governs the development, acquisition, implementation, and maintenance of application development and enhancement projects.

Changes to the production environment are documented within a ticketing system and require approval prior to implementation. Additionally, application changes require documented testing to be performed by QA personnel on an as needed basis, and back out plans are documented on an as needed basis for infrastructure changes prior to being implemented.

Separate environments are maintained for the development and testing purposes from the production environment. OneTrust uses non-production data (fictitious data) within the development and testing environments. Changes are migrated to production by authorized personnel based on job responsibilities. Logging is enabled to monitor activities such as administrative activities, logon attempts, changes to functions, security configurations, permissions, and roles. Automated alerts are configured to notify IT management and issues identified are resolved in a timely manner through the incident management process.

Release notes for changes that affect the system are documented and communicated to internal and external users.

System Security and System Monitoring

OneTrust utilizes a web application firewall is also in place and is configured to protect against external web-based attacks. Anti-malware software is deployed on production servers and workstations and is configured to scan registered endpoints in real-time. A Data Loss Prevention (DLP) application is configured to prevent the use of removable media devices on registered endpoints. Additionally, an Intrusion Detection System (IDS) tool is configured to notify system administrators of potential unauthorized movement of sensitive information.

In order to help ensure production capacity is adequate, OneTrust utilizes enterprise monitoring software to monitor system capacity, and availability issues are configured to alert cloud personnel when pre-defined thresholds are met. System changes are implemented as needed to help ensure that processing capacity can meet demand.

Incident Response

OneTrust maintains an incident response program to guide personnel on identifying, reporting, and tracking security incidents. OneTrust utilizes an incident reporting tool to escalate identified security incidents. A compliance and fraud reporting hotline is in place for employees to report security incidents or unethical behaviors anonymously, and a ticketing system is utilized to prioritize and track incidents and issues. Incidents related to security, availability, and confidentiality are logged, tracked, and communicated to affected parties (where applicable) by management until resolution. Incidents are evaluated to determine whether they could have resulted in a failure to meet security, availability, and confidentiality commitments and objectives.

Data Backup, Disaster Recovery, and Business Disruption Management

OneTrust employs multiple methods to ensure high availability of systems for end users. Backup restore points are created and stored to ensure the availability of customer data in the event that data loss occurs. Databases are replicated to a secondary region in real time. Backup restoration testing is performed on an annual basis to test the integrity and completeness of back-up information. The incident management process is invoked for anomalies. Additionally, a multi-location strategy is employed for production environment to permit the resumption of operations at other availability zones in the event of the loss of a facility. Documented procedures outline the process that the

Company’s staff follows to back up and recover customer data. The procedures are reviewed by management at least annually.

A disaster recovery production environment is maintained within AWS that is geographically separated from the main production environment. A disaster recovery program is in place to protect the infrastructure in the occurrence of an adverse event that can impact operations and this plan is tested annually. The business continuity plan is tested at least on an annual basis and recommendations and actions are documented. A documented business continuity plan is in place and is tested at least on an annual basis and recommendations and actions are documented.

To manage risks associated with business disruptions, A business impact analysis is performed on an annual basis to determine and evaluate the effects of an interruption to critical business operations. This business impact analysis informs OneTrust on their strategies for system redundancy and recovery plans.

Vendor Management

Procedures for managing the risks associated with engaging with third parties, such as vendors. Management obtains and reviews the subservice organization’s third-party compliance reports on an annual basis. Additionally, a vendor risk assessment is performed at least annually for critical vendors. Exceptions or concerns noted in the vendor risk assessments or vendor risk assessments are evaluated to determine impact on service.

Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by OneTrust. Through the API, the customer or end user defines and controls the data they load into and store in the Certification Automation system production environment. Once stored in the environment, the data is accessed remotely from customer systems via the internet.

Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in client contracts and in accordance with the OneTrust’s Classification Standards.

OneTrust has deployed secure methods and protocols for the transmission of confidential or sensitive information over public networks. Data transmitted through public networks is encrypted utilizing acceptable industry standards. The connection between the database and the application servers is not encrypted but occurs in a private and secure subnet.

The Certification Automation system collects the following information:

- User information – Typically keeps track of the name and e-mail address assigned to the system to create a user account.
- Usage information –Tracks user activity in relation to the types of services customers and their users use, the configuration of their computers, and performance metrics related to their use of the services.
- Log information – Logs system activity, including Internet Protocol (IP) address.
- Information collected by cookies and similar technologies – OneTrust uses various technologies to collect information that may include saving cookies to users’ computers.

The Certification Automation system provides a system that forms a system of record for the Information Security Management System of an enterprise. This solution collects data only from authorized users and does not collect any data from public sources, social media, or the Internet. The Certification Automation system may collect data from other enterprise systems but only via partner APIs and authorized users.

System boundaries pertaining to collection, use, retention, disclosure, and disposal or anonymization, or personalization of data are governed by contract provisions for particular service engagements. Data is not utilized or disclosed to third parties outside of the scope allowed in such contracts and agreements.

Significant Changes During the Period

There were no significant changes that are likely to affect report users' understanding of how the in-scope system is used to provide the services covered by this examination during the period.

Subservice Organizations

The cloud hosting and managed database services provided by AWS were not included within the scope of this examination.

The following table presents the applicable Trust Services criteria that are intended to be met by controls at AWS, alone or in combination with controls at OneTrust, and the types of controls expected to be implemented at AWS to achieve OneTrust's principal service commitments and system requirements based on the applicable trust services criteria.

Ref.	Control Activities Expected to be Implemented by AWS	Applicable Trust Services Criteria
CSOC1	AWS is expected to implement control activities to manage logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where in-scope systems reside. AWS is also expected to implement control activities for managing logical access to database server operating systems for its cloud hosting services where in-scope systems reside.	CC6.1 - CC6.3, CC6.6
CSOC2	AWS is expected to implement control activities that ensure physical access to facilities, backup media, and other system components including firewalls, routers, and servers is restricted to authorized personnel.	CC6.4 - CC6.5
CSOC3	AWS is expected to implement control activities that ensure environmental protection controls are in place at facilities housing production infrastructure and backup media where in-scope systems reside.	A1.2

Control Environment

The control environment at OneTrust is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment factors include the integrity and ethical values; management's commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided by executive management and operations management.

Integrity and Ethical Values

A "tone at the top" is established by OneTrust, including explicit guidance about what is right and wrong. This tone is communicated and practiced by executives and management throughout the organization. The importance of high ethics and controls is discussed with newly hired employees throughout the interview process and orientation. Employees must acknowledge the employee handbook upon hire, which describes the responsibilities and expected behavior with regard to data and information system usage. New employees are also subjected to background and reference checks prior to joining the organization. A formalized whistleblower policy is established, and an anonymous communication channel is available for employees to report potential security issues or fraud concerns.

Executive Management, Board of Directors, and Audit Committee Oversight

The IMS Committee has been appointed to provide oversight for the development and performance of internal control. The committee meets on a quarterly basis and maintains formal meeting minutes. The IMS Committee responsibilities, inclusive of the establishment, implementation, maintenance, and continual improvement of the IMS, are documented within the information security policy. These responsibilities include ensuring that information security and privacy policies and objectives are established and compatible with the strategic direction of the company. The chair of the IMS Committee is responsible for reporting performance to OneTrust's CEO and others, as relevant.

The organization also performs an internal audit on an annual basis to ensure compliance with organizational policies and procedures and to identify new risks.

OneTrust's Board of Directors consists of the CEO and three independent non-employee directors. The Board provides strategic direction and drives accountability, while overseeing the governance, compliance, reporting, and financials of the organization.

Organizational Structure and Assignment of Authority and Responsibility

OneTrust has established lines of reporting that facilitate the flow of information to appropriate personnel. Roles and responsibilities are segregated based on functional requirements. OneTrust has documented an organization chart that sets forth the company's lines of reporting and is updated as necessary.

Management and employees are assigned levels of authority and responsibility to facilitate effective internal control.

Commitment to Competence

OneTrust's has established a framework for the basic skills necessary to perform each of the jobs at OneTrust. This framework is then augmented with more specific requirements for each position and for additional specialization within each position based upon any other skills an employee may have. Job descriptions are documented for employees to define the skills and knowledge levels required for the competence levels of jobs. Candidates looking to work at the company are assessed during interviewing to determine if their skills match the requirements of the position and to determine if the candidate fits the company culture. Management is required to provide feedback to HR during candidate interviewing to assess the competency of the candidate prior to being offered a position. New employees are subjected to background and reference checks prior to joining the organization. Employees are also required to undergo mandatory security and privacy training upon hire, and on an annual basis thereafter. Employees' performance is also evaluated by managers on at least an annual basis.

Accountability

OneTrust's senior management takes a "hands on" approach and are heavily involved in all phases of business operations. OneTrust has company-wide staff meetings on a quarterly basis that enable senior management to remain in close contact with all personnel and to consistently emphasize appropriate behavior to personnel and to key vendor personnel.

OneTrust maintains formal hiring, employment, and termination policies and procedures. Employees are subject to background checks, must successfully complete privacy and security training, and are subject to disciplinary action as a result of policy violations or acts that are deemed contrary to the company's mission and objectives. Job descriptions are documented for employees to define the knowledge and skillset required for the competence levels of jobs.

RISK ASSESSMENT

Objective Setting

OneTrust identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how to manage them. Documented policies and procedures are in place to guide personnel when performing the risk assessment process. The process incorporates the security program by reviewing security testing and include items that need remediation. Management has committed to customers to carry out certain objectives in relation to the services provided. OneTrust has a risk assessment process to identify and manage risks that could affect the company's ability to provide reliable services to its clients. This process requires management to identify significant risks in their areas of responsibility and to implement measures to address those risks. In designing its controls, the company has considered the risks that could prevent it from effectively addressing the criteria under the security, availability, and confidentiality Trust Services Criteria. As part of this process, threats and changes to service commitments are identified and the risks are formally assessed. A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.

Risk Identification and Analysis

After objectives have been defined, risks are identified. The risk identification process includes the consideration of both internal and external factors and their impact on the achievement of the objectives.

OneTrust identifies and assesses changes that could significantly impact the system of internal control. The risk identification process considers changes to the regulatory, economic, and physical environment in which the company operates. OneTrust also considers the potential impacts of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations, rapid growth, and new technologies on the system of internal control.

Subsequently, identified risks are analyzed through a process that includes estimating the potential significance of the risk. Risks are assigned a score based on the combined level of impact and likelihood of the risk occurring, ranging from low to critical impact and unlikely to expected likelihood. Risks are then formally documented with mitigation strategies for management review.

Risk Factors

Management considers risks that can arise from both external and internal factors including the following:

External Factors

- Technological developments
- Competition that could alter marketing or service activities
- New legislation and regulation that could force changes in policies and strategies
- Economic changes that could have an impact on management decisions

Internal Factors

- Significant changes in policies, processes, or personnel
- Types of fraud
- Fraud incentives and pressures for employees
- Fraud opportunities

- Employee attitudes and rationalizations for fraud
- A disruption in information systems processing

Potential for Fraud

OneTrust considers the potential for fraud in assessing risks to the achievement of objectives. The assessment of fraud risk considers fraudulent reporting, possible loss of assets, or data and corruption resulting from the various ways that fraud and misconduct can occur. It also considers opportunities for unauthorized acquisition, use or disposal of assets, altering of the entity's reporting records, or committing other inappropriate acts and how management and other personnel might engage in or justify inappropriate actions.

Risk Mitigation

Documented policies and procedures are in place to guide personnel in identifying and selecting and developing risk management strategies as a component of the annual risk assessment. Upon completion of the annual risk assessment, OneTrust has implemented a risk mitigation procedure for the risks identified during the risk assessment. Risks are documented with mitigation strategies and are reviewed during the quarterly IMS Management Committee quarterly meetings.

Trust Services Criteria and Related Control Activities

Integration with Risk Assessment

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of the security, availability, and confidentiality categories.

Selection and Development of Control Activities

The applicable trust services criteria and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in Section 4. Although the applicable trust services criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of OneTrust's description of the system.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4, the Testing Matrices, adjacent to the service organization's description of controls. 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.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security, availability, and confidentiality categories are applicable to the Certification Automation system.

Information and Communication Systems

OneTrust obtains or generates and uses relevant information to support the functioning of internal control. OneTrust maintains architectural diagrams and procedural documentation to allow for identification of data sources, responsible personnel, and other relevant information. OneTrust has methods in place to help information systems maintain and produce information that is timely, current, accurate, and complete.

Internal Communications

OneTrust maintains information security policies to help ensure that employees understand their individual roles and responsibilities concerning processing and controls to ensure significant events are communicated in a timely manner. These include training programs and the use of e-mail to communicate time sensitive information and processes for security and system availability purposes that notify key personnel in the event of potential security issues or system outages.

External Communications

OneTrust provides external users with guidelines and technical support resources relating to system operations on OneTrust's website. OneTrust provides an external-facing support system and contact information to allow users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel. OneTrust notifies customers of critical changes that may affect their processing.

Monitoring

Monitoring is a process that assesses the quality of internal control performance over time. It involves assessing the design and operation of controls and taking necessary corrective actions. This process is accomplished through ongoing activities, separate evaluation, or a combination of the two. Monitoring activities also include using information from communications from external parties such as user entity complaints and regulatory comments that may indicate problems or highlight areas in need of improvement. Management has implemented a self-assessment and compliance program to ensure the controls are consistently applied as designed.

Ongoing Monitoring

OneTrust's management performs monitoring activities in order to assess the quality of internal control over time, monitors activities throughout the year, and takes corrective actions to address deviations from company policy and procedures. Management utilizes a risk-based approach to monitor business units and other auditable entities throughout the organization, ensuring that enterprise-wide risks are prioritized and addressed in order of significance.

OneTrust monitors customer communications through the Professional Services and Support department. This information is provided to management providing the ability to track, monitor, and assist in understanding customer complaints, concerns, and to evaluate and resolve special requests in a timely fashion. Management's ability to actively monitor customer communications is an integral role in controlling the quality of the services provided.

Management is proactive in responding to customer complaints and there is a high level of inter-departmental communication about these events. Customer complaints and other issues are handled through an internal ticketing system and by personal contact by management staff. Major customer-facing issues are reported to management for discussion and approval of action.

OneTrust utilizes monitoring tools to monitor system security and performance events such as failed access attempts, intrusion signature detection, firewall events, central processing unit (CPU), and memory usage. Monitoring systems are configured to notify personnel when pre-defined thresholds are met and are followed up with and remediated.

Separate Evaluations

The IMS Committee is responsible for providing oversight for the development and performance of internal controls. The committee meets on a quarterly basis to review security incidents and various other metrics to determine the effectiveness of internal controls. Additionally, the organization performs an internal audit on an annual basis to ensure compliance with organizational policies and procedures and to identify new risks. Vulnerability scans are performed on a daily basis to identify threats and vulnerabilities to the production systems. Issues identified are analyzed and remediated in a timely manner. OneTrust also contracts with a third-party to perform penetration testing on an annual basis to identify vulnerabilities and deficiencies.

Subservice Organization Monitoring

The externally supported systems managed by AWS that support the Certification Automation system are monitored daily by OneTrust IT personnel as part of the day-to-day IT and business operations. Vendor risk assessments are performed at least annually for critical vendors, and any exceptions identified in the assessment are evaluated to determine the impact on service. OneTrust also obtains and reviews third-party attestation and compliance reports for AWS on at least an annual basis to monitor and evaluate the adequacy and effectiveness of controls in place at the subservice organization to safeguard client data.

Evaluating and Communicating Deficiencies

OneTrust evaluates and communicates internal control deficiencies to those parties responsible for taking corrective action, including senior management and the board of managers, as appropriate. Guidelines for reporting deficiencies have been developed and are provided to all employees. The IMS Committee meets on a quarterly basis to review reported security incidents.

There were no identified significant system incidents that (a) were the result of controls that were not suitably designed or operating effectively to achieve one or more of the service commitments and system requirements or (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements during the period.

System Incident Disclosures

No system incidents occurred that were the result of controls that were not suitably designed or operating effectively or otherwise resulted in a significant failure of the achievement of one or more of the service commitments and systems requirements during the period.

Complementary Controls at User Entities

OneTrust's controls are designed to provide reasonable assurance that the principal service commitments and system requirements can be achieved without the implementation of complementary controls at user entities. As a result, complementary user entity controls are not required, or significant, to achieve the principal service commitments and system requirements based on the applicable trust services criteria.

SECTION 4

TESTING MATRICES

Tests of Operating Effectiveness and Results of Tests

Scope of Testing

This report on the controls relates to the Certification Automation system provided by OneTrust. The scope of the testing was restricted to the Certification Automation system and its boundaries as defined in Section 3. Schellman conducted the examination testing over the period May 1, 2024, through April 30, 2025.

Tests of Operating Effectiveness

The tests applied to test the operating effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the applicable trust services criteria were achieved during the period. In selecting the tests of controls, Schellman considered various factors including, but not limited to, the following:

- the nature of the control and the frequency with which it operates;
- the control risk mitigated by the control;
- the effectiveness of entity-level controls, especially controls that monitor other controls;
- the degree to which the control relies on the effectiveness of other controls; and
- whether the control is manually performed or automated.

The types of tests performed with respect to the operational effectiveness of the control activities detailed in this section are briefly described below:

Test Approach	Description
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Observation	Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Inspection	Inspected the relevant audit records. This included, but was not limited to, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing events forward to consequent system documentation or processes (e.g., resolution, detailed documentation, alarms, etc.) or vouching backwards for prerequisite events (e.g., approvals, authorizations, etc.).

Sampling

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, Schellman utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, in order to determine the number of items to be selected in a sample for a particular test. Schellman, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

Reliability of Information Provided by the Service Organization

Observation and inspection procedures were performed related to certain system-generated reports, listings, and queries to assess the accuracy and completeness (reliability) of the information used in the performance of our testing of the controls.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase "No exceptions noted." in the test result column of the Testing Matrices. Any phrase other than the aforementioned, constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the operating effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors. Control considerations that should be implemented by subservice organizations, in order to complement the control activities and achieve the applicable trust services criteria are presented in the "Subservice Organizations" section within Section 3.

Security Category

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Control Environment			
CC1.1 – COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	Employees must acknowledge the employee handbook upon hire, which describes the responsibilities and expected behavior with regard to data and information system usage.	Inspected the listing of employees hired during the period and the query used to generate the listing and determined that no employees were hired during the period; therefore, no testing of operating effectiveness was performed.	
CC1.1.2	A formalized whistleblower policy is established and an anonymous communication channel is available for employees to report potential security issues or fraud concerns.	Inspected the whistleblower policy and the communication channel on the Company website to determine that a formalized whistleblower policy was established and an anonymous communication channel was available for employees to report potential security issues or fraud concerns.	No exceptions noted.
CC1.1.3	New employees are subjected to background checks prior to joining the organization.	Inspected the listing of employees hired during the period and the query used to generate the listing and determined that no employees were hired during the period; therefore, no testing of operating effectiveness was performed.	

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.1.4	Employees and contractors who violate the code of conduct are subject to disciplinary actions documented in the employee handbook.	Inspected the employee handbook to determine that employees and contractors who violate the code of conduct were subject to disciplinary actions.	No exceptions noted.
CC1.2 – COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2.1	IMS Management Committee responsibilities, inclusive of the establishment, implementation, maintenance, and continual improvement of the IMS, are documented within the information security policy.	Inspected the information security policy to determine that the IMS Management Committee responsibilities, inclusive of the establishment, implementation, maintenance, and continual improvement of the IMS, were documented within the information security policy.	No exceptions noted.
CC1.2.2	The IMS Management Committee is comprised of an appointed IMS chair and supporting leadership members.	Inspected the information security policy to determine that the IMS Management Committee was comprised of an appointed IMS chair and supporting leadership members.	No exceptions noted.
CC1.2.3	The IMS Management Committee has been appointed to provide oversight for the development and performance of internal control. The committee meets at least quarterly and maintains formal meeting minutes.	Inspected the executive team meeting minutes for a sample of quarters during the period to determine that the IMS Management Committee was appointed to provide oversight for the development and performance of internal control and that the committee met quarterly and maintained formal meeting minutes.	No exceptions noted.
CC1.3 – COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3.1	The IMS Management Committee has been appointed to provide oversight for the development and performance of internal control. The committee meets at least quarterly and maintains formal meeting minutes.	Inspected the executive team meeting minutes for a sample of quarters during the period to determine that the IMS Management Committee was appointed to provide oversight for the development and performance of internal control and that the committee met quarterly and maintained formal meeting minutes.	No exceptions noted.
CC1.3.2	Job descriptions are documented for employees to define the skills and knowledge levels required for the competence levels of jobs.	Inspected the documented job description for a sample of unique job positions from the current employee listing to determine that job descriptions were documented for employees and defined the skills and knowledge levels required for the competence levels of jobs for each job position sampled.	No exceptions noted.

<table>
<tr><th>Control #</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>CC1.3.3</td><td>An organization chart is documented and defines the organizational structure and reporting lines.</td><td>Inspected the organizational chart to determine that an organization chart was documented and defines the organizational structure and reporting lines.</td><td>No exceptions noted.</td></tr>
<tr><td>CC1.3.4</td><td>Management has established defined roles and responsibilities to oversee the implementation of security and internal controls.</td><td>Inspected the information security policy documentation to determine that management established defined roles and responsibilities to oversee the implementation of security and internal controls.</td><td>No exceptions noted.</td></tr>
<tr><td colspan="4">CC1.4 – COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.</td></tr>
<tr><td>CC1.4.1</td><td>The organization has implemented a process that requires managers to evaluate employee performance on at least an annual basis.</td><td>Inspected the completed performance evaluation for a sample of current employees to determine that the organization has implemented a process that requires managers to evaluate employee performance on at least an annual basis.</td><td>No exceptions noted.</td></tr>
<tr><td rowspan="2">CC1.4.2</td><td rowspan="2">Employees complete security awareness training upon hire and annually thereafter.</td><td>Inspected the training documentation for a sample of current employees to determine that employees completed security awareness training annually.</td><td>No exceptions noted.</td></tr>
<tr><td colspan="2">Inspected the listing of employees hired during the period and the query used to generate the listing and determined that no employees were hired during the period; therefore, no testing of operating effectiveness was performed.</td></tr>
<tr><td>CC1.4.3</td><td>New employees are subjected to background checks prior to joining the organization.</td><td colspan="2">Inspected the listing of employees hired during the period and the query used to generate the listing and determined that no employees were hired during the period; therefore, no testing of operating effectiveness was performed.</td></tr>
<tr><td>CC.1.4.4</td><td>Job descriptions are documented for employees to define the skills and knowledge levels required for the competence levels of jobs.</td><td>Inspected the documented job description for a sample of unique job positions from the current employee listing to determine that job descriptions were documented for employees and defined the skills and knowledge levels required for the competence levels of jobs for each job position sampled.</td><td>No exceptions noted.</td></tr>
<tr><td colspan="4">CC1.5 – COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.</td></tr>
<tr><td>CC1.5.1</td><td>The organization has implemented a process that requires managers to evaluate employee performance on at least an annual basis.</td><td>Inspected the completed performance evaluation for a sample of current employees to determine that the organization has implemented a process that requires managers to evaluate employee performance on at least an annual basis.</td><td>No exceptions noted.</td></tr>
</table>

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.5.2	Employees must acknowledge the employee handbook upon hire, which describes the responsibilities and expected behavior with regard to data and information system usage.	Inspected the listing of employees hired during the period and the query used to generate the listing and determined that no employees were hired during the period; therefore, no testing of operating effectiveness was performed.	
CC1.5.3	Employees and contractors who violate the code of conduct are subject to disciplinary actions documented in the employee handbook.	Inspected the employee handbook to determine that employees and contractors who violate the code of conduct were subject to disciplinary actions.	No exceptions noted.
CC1.5.4	An internal audit is performed at least annually to validate that controls are in place and operating effectively. Internal control deficiencies are communicated to parties responsible for taking corrective action.	Inspected the most recent internal audit results to determine that an internal audit was performed during the period to validate that controls were in place and operated effectively and that internal control deficiencies were communicated to parties responsible for taking corrective action.	No exceptions noted.
Communication and Information			
CC2.1 – COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	An internal audit is performed at least annually to validate that controls are in place and operating effectively. Internal control deficiencies are communicated to parties responsible for taking corrective action.	Inspected the most recent internal audit results to determine that an internal audit was performed during the period to validate that controls were in place and operated effectively and that internal control deficiencies were communicated to parties responsible for taking corrective action.	No exceptions noted.
CC2.1.2	The security owners subscribe to industry security bulletins and e-mail alerts and use them to monitor the impact of emerging technologies and security on the production systems.	Inspected example security bulletins and e-mail alerts to determine that the security owners were subscribed to industry security bulletins and e-mail alerts and used them to monitor the impact of emerging technologies and security on the production systems.	No exceptions noted.
CC2.1.3	Vulnerability scans are performed on a daily basis to identify threats and vulnerabilities to the production systems. Issues identified are analyzed and remediated in a timely manner.	Inspected the vulnerability dashboard and configuration to determine that vulnerability scans were performed on a daily basis to identify threats and vulnerabilities to the production systems.	No exceptions noted.
		Inspected an example remediation ticket to determine that issues identified were analyzed and remediated in a timely manner.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.1.4	A third-party penetration test is performed on an annual basis to identify vulnerabilities and deficiencies. Remediation plans are proposed and monitored through resolution.	Inspected the penetration test to determine that a third-party penetration test was performed during the period to identify vulnerabilities and deficiencies.	No exceptions noted.
		Inspected a remediation ticket to determine that remediation plans were proposed and monitored through resolution.	No exceptions noted.
CC2.2 – COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.2.1	Information security policies and procedures are documented and define the information security rules and requirements for the service environment.	Inspected the information security policies and procedures to determine that information security policies and procedures were documented and defined the information security rules and requirements for the service environment.	No exceptions noted.
CC2.2.2	The organization utilizes OneTrust platform to manage its Information Security policies and procedures. Internal policy and procedure documents relating to security, confidentiality, and availability are maintained and made available to employees. The policies and procedure documents are reviewed and approved by management annually or during significant changes.	Inspected the information security policies and procedures shared on the OneTrust platform to determine that the Company utilized the OneTrust platform to manage its information security policies and procedures related to security, confidentiality, and availability and were maintained and made available to employees.	No exceptions noted.
		Inspected the information security policies on the company intranet to determine that documents were reviewed and approved by management annually or during significant changes.	No exceptions noted.
CC2.2.3	Guidelines and technical support resources related to system operations are provided to internal and external users on the Company's website.	Inspected the guidelines and technical support resources on the Company website to determine that guidelines and technical support resources related to system operations were provided to internal and external users on the Company's website.	No exceptions noted.
CC2.2.4	Release notes for changes that affect the system are documented and communicated to internal and external users.	Inspected the release notes webpage to determine that release notes for changes that affected the system were documented and communicated to internal and external users.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2.5	Security incident response policies and procedures are documented and provide guidance to Company personnel for detecting, responding to, and recovering from security events and incidents.	Inspected the incident response policies and procedures to determine that security incident response policies and procedures were documented and provided guidance to company personnel for detecting, responding to, and recovering from security events and incidents.	No exceptions noted.
CC2.2.6	Management has established defined roles and responsibilities to oversee the implementation of security and internal controls.	Inspected the information security policy documentation to determine that management established defined roles and responsibilities to oversee the implementation of security and internal controls.	No exceptions noted.
CC2.2.7	A formalized whistleblower policy is established and an anonymous communication channel is available for employees to report potential security issues or fraud concerns.	Inspected the whistleblower policy and the communication channel on the Company website to determine that a formalized whistleblower policy was established and an anonymous communication channel was available for employees to report potential security issues or fraud concerns.	No exceptions noted.
CC2.2.8	Employees must acknowledge the employee handbook upon hire, which describes the responsibilities and expected behavior with regard to data and information system usage.	Inspected the listing of employees hired during the period and the query used to generate the listing and determined that no employees were hired during the period; therefore, no testing of operating effectiveness was performed.	
CC2.2.9	Employees complete security awareness training upon hire and annually thereafter.	Inspected the training documentation for a sample of current employees to determine that employees completed security awareness training annually.	No exceptions noted.
		Inspected the listing of employees hired during the period and the query used to generate the listing and determined that no employees were hired during the period; therefore, no testing of operating effectiveness was performed.	
CC2.2.10	Employees are required to sign a confidentiality agreement upon hire. This agreement prohibits any disclosure of information and other data to which the employee has been granted access during employment and after termination.	Inspected the listing of employees hired during the period and the query used to generate the listing and determined that no employees were hired during the period; therefore, no testing of operating effectiveness was performed.	

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2.11	The IMS Management Committee has been appointed to provide oversight for the development and performance of internal control. The committee meets at least quarterly and maintains formal meeting minutes.	Inspected the executive team meeting minutes for a sample of quarters during the period to determine that the IMS Management Committee was appointed to provide oversight for the development and performance of internal control and that the committee met quarterly and maintained formal meeting minutes.	No exceptions noted.
CC2.3 – COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	The master terms of service and service level agreements include the communication of the Company's commitments to its customers.	Inspected the terms of service to determine that the master terms of service and service level agreements included the communication of the Company's commitments to its customers.	No exceptions noted.
CC2.3.2	Data protection agreements are in place with third-party vendors. These agreements include confidentiality commitments applicable to that entity.	Inspected the service terms and customer agreement for a sample of critical vendors to determine that data protection agreements were in place with third-party vendors and that these agreements included confidentiality commitments applicable to that entity.	No exceptions noted.
CC2.3.3	Guidelines and technical support resources related to system operations are provided to internal and external users on the Company's website.	Inspected the guidelines and technical support resources on the Company website to determine that guidelines and technical support resources related to system operations were provided to internal and external users on the Company's website.	No exceptions noted.
CC2.3.4	Release notes for changes that affect the system are documented and communicated to internal and external users.	Inspected the release notes webpage to determine that release notes for changes that affected the system were documented and communicated to internal and external users.	No exceptions noted.
CC2.3.5	An external-facing support system is in place that allows external users to report system information on failures, incidents, concerns, and other complaints to the company.	Inspected the customer support tickets for a sample of help desk tickets resolved during the period to determine that that an external-facing support system was in place that allowed external users to report system information on failures, incidents, concerns, and other complaints to the company.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Risk Assessment			
CC3.1 – COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	A documented risk methodology program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk methodology document to determine that a documented risk management program was in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks	No exceptions noted.
CC3.1.2	A formal risk assessment process is performed on at least an annual basis. Risks that are identified are rated using a risk evaluation process and are formally documented, with mitigation strategies for management review.	Inspected the documentation for the most recently completed risk assessment to determine that a risk assessment was performed during the period and that identified risks were rated using a risk evaluation process and were formally documented, with mitigation strategies for management review.	No exceptions noted.
CC3.2 – COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC3.2.1	A documented risk methodology program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk methodology document to determine that a documented risk management program was in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks	No exceptions noted.
CC3.2.2	A formal risk assessment process is performed on at least an annual basis. Risks that are identified are rated using a risk evaluation process and are formally documented, with mitigation strategies for management review.	Inspected the documentation for the most recently completed risk assessment to determine that a risk assessment was performed during the period and that identified risks were rated using a risk evaluation process and were formally documented, with mitigation strategies for management review.	No exceptions noted.
CC3.3 – COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	A risk assessment is performed on an annual basis that considers the potential for fraud.	Inspected the documentation for the most recently completed risk assessment to determine that a risk assessment was performed during the period and that considered the potential for fraud.	No exceptions noted.

Control #	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.			
CC3.4.1	A documented risk methodology program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk methodology document to determine that a documented risk management program was in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks	No exceptions noted.
CC3.4.2	A formal risk assessment process is performed on at least an annual basis. Risks that are identified are rated using a risk evaluation process and are formally documented, with mitigation strategies for management review.	Inspected the documentation for the most recently completed risk assessment to determine that a risk assessment was performed during the period and that identified risks were rated using a risk evaluation process and were formally documented, with mitigation strategies for management review.	No exceptions noted.
CC3.4.3	An internal audit is performed at least annually to validate that controls are in place and operating effectively. Internal control deficiencies are communicated to parties responsible for taking corrective action.	Inspected the most recent internal audit results to determine that an internal audit was performed during the period to validate that controls were in place and operated effectively and that internal control deficiencies were communicated to parties responsible for taking corrective action.	No exceptions noted.
Monitoring Activities			
CC4.1 – COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1.1	The IMS Management Committee has been appointed to provide oversight for the development and performance of internal control. The committee meets at least quarterly and maintains formal meeting minutes.	Inspected the executive team meeting minutes for a sample of quarters during the period to determine that the IMS Management Committee was appointed to provide oversight for the development and performance of internal control and that the committee met quarterly and maintained formal meeting minutes.	No exceptions noted.
CC4.1.2	An internal audit is performed at least annually to validate that controls are in place and operating effectively. Internal control deficiencies are communicated to parties responsible for taking corrective action.	Inspected the most recent internal audit results to determine that an internal audit was performed during the period to validate that controls were in place and operated effectively and that internal control deficiencies were communicated to parties responsible for taking corrective action.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.1.3	Management obtains and reviews the subservice organizations third-party compliance reports on an annual basis.	Inspected the attestation reports and the completed risk assessments for a sample of critical vendors engaged with throughout the period to determine that management obtained and reviewed the subservice organization's third-party compliance reports during the period.	No exceptions noted.
CC4.1.4	Vulnerability scans are performed on a daily basis to identify threats and vulnerabilities to the production systems. Issues identified are analyzed and remediated through resolution.	Inspected the vulnerability dashboard and configuration to determine that vulnerability scans were performed on a daily basis to identify threats and vulnerabilities to the production systems.	No exceptions noted.
		Inspected a remediation ticket to determine that remediation plans were proposed and monitored through resolution.	No exceptions noted.
CC4.1.5	A third-party penetration test is performed on an annual basis to identify vulnerabilities and deficiencies. Remediation plans are proposed and monitored through resolution.	Inspected the penetration test to determine that a third-party penetration test was performed during the period to identify vulnerabilities and deficiencies.	No exceptions noted.
		Inspected a remediation ticket to determine that remediation plans were proposed and monitored through resolution.	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.			
CC4.2.1	The IMS Management Committee has been appointed to provide oversight for the development and performance of internal control. The committee meets at least quarterly and maintains formal meeting minutes.	Inspected the executive team meeting minutes for a sample of quarters during the period to determine that the IMS Management Committee was appointed to provide oversight for the development and performance of internal control and that the committee met quarterly and maintained formal meeting minutes.	No exceptions noted.
CC4.2.2	An internal audit is performed at least annually to validate that controls are in place and operating effectively. Internal control deficiencies are communicated to parties responsible for taking corrective action.	Inspected the most recent internal audit results to determine that an internal audit was performed during the period to validate that controls were in place and operated effectively and that internal control deficiencies were communicated to parties responsible for taking corrective action.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.2.3	Management obtains and reviews the subservice organizations third-party compliance reports on an annual basis.	Inspected the attestation reports and the completed risk assessments for a sample of critical vendors engaged with throughout the period to determine that management obtained and reviewed the subservice organization's third-party compliance reports during the period.	No exceptions noted.
CC4.2.4	Incidents related to security, availability, and confidentiality are logged, tracked, and communicated to affected parties (where applicable) by management until resolved. Incidents are evaluated to determine whether they could have resulted in a failure to meet security, availability, and confidentiality commitments and objectives.	Inspected the incident ticket and communication documentation for a listing of incidents reported during the period to determine that for each incident sampled, incidents were logged, tracked, and communicated to affected parties by management until resolved and that incidents were evaluated to determine whether they could have resulted in a failure to meet security, availability, and confidentiality commitments and objectives.	No exceptions noted.
Control Activities			
CC5.1 – COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC5.1.1	A documented risk methodology program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk methodology document to determine that a documented risk management program was in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks	No exceptions noted.
CC5.1.2	A formal risk assessment process is performed on at least an annual basis. Risks that are identified are rated using a risk evaluation process and are formally documented, with mitigation strategies for management review.	Inspected the documentation for the most recently completed risk assessment to determine that a risk assessment was performed during the period and that identified risks were rated using a risk evaluation process and were formally documented, with mitigation strategies for management review.	No exceptions noted.
CC5.1.3	An internal audit is performed at least annually to validate that controls are in place and operating effectively. Internal control deficiencies are communicated to parties responsible for taking corrective action.	Inspected the most recent internal audit results to determine that an internal audit was performed during the period to validate that controls were in place and operated effectively and that internal control deficiencies were communicated to parties responsible for taking corrective action.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.1.4	The IMS Management Committee has been appointed to provide oversight for the development and performance of internal control. The committee meets at least quarterly and maintains formal meeting minutes.	Inspected the executive team meeting minutes for a sample of quarters during the period to determine that the IMS Management Committee was appointed to provide oversight for the development and performance of internal control and that the committee met quarterly and maintained formal meeting minutes.	No exceptions noted.
CC5.2 – COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	A documented risk methodology program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk methodology document to determine that a documented risk management program was in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks	No exceptions noted.
CC5.2.2	A formal risk assessment process is performed on at least an annual basis. Risks that are identified are rated using a risk evaluation process and are formally documented, with mitigation strategies for management review.	Inspected the documentation for the most recently completed risk assessment to determine that a risk assessment was performed during the period and that identified risks were rated using a risk evaluation process and were formally documented, with mitigation strategies for management review.	No exceptions noted.
CC5.2.3	An internal audit is performed at least annually to validate that controls are in place and operating effectively. Internal control deficiencies are communicated to parties responsible for taking corrective action.	Inspected the most recent internal audit results to determine that an internal audit was performed during the period to validate that controls were in place and operated effectively and that internal control deficiencies were communicated to parties responsible for taking corrective action.	No exceptions noted.
CC5.2.4	The IMS Management Committee has been appointed to provide oversight for the development and performance of internal control. The committee meets at least quarterly and maintains formal meeting minutes.	Inspected the executive team meeting minutes for a sample of quarters during the period to determine that the IMS Management Committee was appointed to provide oversight for the development and performance of internal control and that the committee met quarterly and maintained formal meeting minutes.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.3 – COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	Information security policies and procedures are documented and define the information security rules and requirements for the service environment.	Inspected the information security policies and procedures to determine that information security policies and procedures were documented and defined the information security rules and requirements for the service environment.	No exceptions noted.
CC5.3.2	The organization utilizes OneTrust platform to manage its Information Security policies and procedures. Internal policy and procedure documents relating to security, confidentiality, and availability are maintained and made available to employees. The policies and procedure documents are reviewed and approved by management annually or during significant changes.	Inspected the information security policies and procedures shared on the OneTrust platform to determine that the Company utilized the OneTrust platform to manage its information security policies and procedures related to security, confidentiality, and availability and were maintained and made available to employees.	No exceptions noted.
		Inspected the information security policies on the company intranet to determine that documents were reviewed and approved by management annually or during significant changes.	No exceptions noted.
CC5.3.3	Security incident response policies and procedures are documented and provide guidance to Company personnel for detecting, responding to, and recovering from security events and incidents.	Inspected the incident response policies and procedures to determine that security incident response policies and procedures were documented and provided guidance to company personnel for detecting, responding to, and recovering from security events and incidents.	No exceptions noted.
CC5.3.4	The IMS Management Committee has been appointed to provide oversight for the development and performance of internal control. The committee meets at least quarterly and maintains formal meeting minutes.	Inspected the executive team meeting minutes for a sample of quarters during the period to determine that the IMS Management Committee was appointed to provide oversight for the development and performance of internal control and that the committee met quarterly and maintained formal meeting minutes.	No exceptions noted.
CC5.3.5	An internal audit is performed at least annually to validate that controls are in place and operating effectively. Internal control deficiencies are communicated to parties responsible for taking corrective action.	Inspected the most recent internal audit results to determine that an internal audit was performed during the period to validate that controls were in place and operated effectively and that internal control deficiencies were communicated to parties responsible for taking corrective action.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Logical and Physical Access Controls			
CC6.1 – The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.1.1	Information security policies and procedures are documented and define the information security rules and requirements for the service environment.	Inspected the information security policies and procedures to determine that information security policies and procedures were documented and defined the information security rules and requirements for the service environment.	No exceptions noted.
CC6.1.2	A formal inventory of production system assets that includes asset owners is maintained, and changes to the inventory are logged.	Inspected the asset inventory listing to determine that a formal inventory of production system assets was maintained, and changes to the inventory were logged.	No exceptions noted.
CC6.1.3	Authentication to the following in-scope systems components requires a unique username and password: • Application production environment • AWS console	Inspected the authentication configurations to determine that authentication to the following in-scope systems components required a unique username and password or authorized SSH keys: • Production environment • AWS console	No exceptions noted.
CC6.1.4	MFA is required for remote access to production systems over an encrypted gateway.	Inspected the MFA configurations and remote authentication process to determine MFA was required for remote access to production systems over an encrypted gateway.	No exceptions noted.
CC6.1.5	Remote access to production systems is permitted to authorized employees only with multi-factor authentication (MFA) over encrypted channels and through IP whitelisting.	Inspected the MFA configurations to determine that remote access to production systems was permitted to authorized employees only with multi-factor authentication (MFA) over encrypted channels and through IP whitelisting.	No exceptions noted.
		Inspected the list of users with remote access to production systems to determine that remote access to production systems was permitted to authorized employees only with multi-factor authentication (MFA) over encrypted channels and through IP whitelisting.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.6	Administrative access to the in-scope system components is restricted to user accounts accessible by authorized personnel commensurate to their job functions: • Network domain • AWS console • Application • Firewall	Inspected the administrative access configurations and administrative listings with the assistance of the senior information security analyst to determine that the administrative access to the following in-scope system components was restricted to user accounts accessible by authorized personnel commensurate to their job functions: • Network domain • AWS console • Application • Firewall	No exceptions noted.
CC6.1.7	The organization uses its cloud provider key management service to encrypt data at rest and to store and manage encryption keys. Access to production access keys is restricted to authorized individuals.	Inspected database encryption configuration to determine that the organization used its cloud provider key management service to encrypt data at rest and to store and manage encryption keys.	No exceptions noted.
CSOC1	AWS is expected to implement control activities to manage logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where in-scope systems reside. AWS is also expected to implement control activities for managing logical access to database server operating systems for its cloud hosting services where in-scope systems reside.		
CC6.2 – Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC6.2.1	Information security policies and procedures are documented and define the information security rules and requirements for the service environment.	Inspected the information security policies and procedures to determine that information security policies and procedures were documented and defined the information security rules and requirements for the service environment.	No exceptions noted.
CC6.2.2	Access to in-scope system components requires a documented access request and manager approval prior to access being provisioned.	Inspected access request tickets for a sample of users with new access to the Certification Automation application to determine that access to in-scope components required a documented access request and manager approval prior to access being provisioned.	No exceptions noted.
CC6.2.3	In the event of a user termination, notification is provided to appropriate teams and access is revoked for employees as part of the termination process.	Inspected the termination tickets for a sample of terminated employees during the period to determine that notification was provided to appropriate teams and access was revoked for employees as part of the termination process.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.2.4	Annual user access reviews for in-scope systems are conducted by management to help ensure that access is restricted to authorized users.	Inspected the annual user access review documentation to determine that management performed annual user access review for in-scope system components to ensure that access was restricted appropriately.	No exceptions noted.
CSOC1	AWS is expected to implement control activities to manage logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where in-scope systems reside. AWS is also expected to implement control activities for managing logical access to database server operating systems for its cloud hosting services where in-scope systems reside.		
CC6.3 – The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
CC6.3.1	Access to in-scope system components requires a documented access request and manager approval prior to access being provisioned.	Inspected access request tickets for a sample of users with new access to the Certification Automation application to determine that access to in-scope components required a documented access request and manager approval prior to access being provisioned.	No exceptions noted.
CC6.3.2	In the event of a user termination, notification is provided to appropriate teams and access is revoked for employees as part of the termination process.	Inspected the termination tickets for a sample of terminated employees during the period to determine that notification was provided to appropriate teams and access was revoked for employees as part of the termination process.	No exceptions noted.
CC6.3.3	Annual user access reviews for in-scope systems are conducted by management to help ensure that access is restricted to authorized users.	Inspected the annual user access review documentation to determine that management performed annual user access review for in-scope system components to ensure that access was restricted appropriately.	No exceptions noted.
CC6.3.4	Administrative access to the in-scope system components is restricted to user accounts accessible by authorized personnel commensurate to their job functions: • Network domain • AWS console • Application • Firewall	Inspected the administrative access configurations and administrative listings with the assistance of the senior information security analyst to determine that the administrative access to the following in-scope system components was restricted to user accounts accessible by authorized personnel commensurate to their job functions: • Network domain • AWS console • Application • Firewall	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.3.5	Access to migrate changes to production is restricted to authorized personnel.	Inspected the list of users with access to migrate changes to production with the assistance of the senior cloud ops engineer to determine that the ability the migrate changes to production was restricted to authorized personnel with relevant job responsibilities.	No exceptions noted.
CSOC1	AWS is expected to implement control activities to manage logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where in-scope systems reside. AWS is also expected to implement control activities for managing logical access to database server operating systems for its cloud hosting services where in-scope systems reside.		
CC6.4 – The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
CSOC2	AWS is expected to implement control activities that ensure physical access to facilities, backup media, and other system components including firewalls, routers, and servers is restricted to authorized personnel.		
CC6.5 – The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
CC6.5.1	Formal data retention and disposal procedures are documented to guide the secure retention and disposal of Company and customer data.	Inspected the asset management policy to determine that formal data retention and disposal procedures were documented to guide the secure retention and disposal of Company and customer data.	No exceptions noted.
CC6.5.2	Electronic media containing confidential information is purged or destroyed, and certificates of destruction are issued for each device destroyed.	Inspected the certificate of destruction for a sample of disposed assets throughout the period to verify data and software stored on equipment was confirmed to removed and rendered unreadable prior to disposal.	No exceptions noted.
CSOC2	AWS is expected to implement control activities that ensure physical access to facilities, backup media, and other system components including firewalls, routers, and servers is restricted to authorized personnel.		
CC6.6 – The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	A current network diagram exists that defines an objective description of the system.	Inspected the network diagram to determine that a formal network diagram existed that defined an objective description of the system.	No exceptions noted.
CC6.6.2	Secure data transmission protocols are used to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the SSL configurations to determine that secure data transmission protocols were used to encrypt confidential and sensitive data when transmitted over public networks.	No exceptions noted.
CC6.6.3	The databases are configured to encrypt data at rest.	Inspected the encryption configurations for customer data stored in S3 buckets to determine that the databases were configured to encrypt data at rest.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.6.4	System components are configured such that the organization and its customers' access is appropriately segmented from other tenant users.	Inspected the system configuration and architecture diagram to determine that system components were configured such that the organization and its customers' access was appropriately segmented from other tenant users.	No exceptions noted.
CC6.6.5	A web application firewall system is in place and is configured to filter unauthorized inbound network traffic from the Internet.	Inspected the security group rules and network ACLs for the production environment to determine that a web application firewall system was in place and was configured to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
CC6.6.6	The IDS tool is configured to prevent the use of removable media devices on registered endpoints.	Inspected the IDS configurations to determine that the IDS tool was configured to prevent the use of removable media devices on registered endpoints.	No exceptions noted.
CSOC1	AWS is expected to implement control activities to manage logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where in-scope systems reside. AWS is also expected to implement control activities for managing logical access to database server operating systems for its cloud hosting services where in-scope systems reside.		
CC6.7 – The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
CC6.7.1	Secure data transmission protocols are used to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the SSL configurations to determine that secure data transmission protocols were used to encrypt confidential and sensitive data when transmitted over public networks.	No exceptions noted.
CC6.7.2	The databases are configured to encrypt data at rest.	Inspected the encryption configurations for customer data stored in S3 buckets to determine that the databases were configured to encrypt data at rest.	No exceptions noted.
CC6.7.3	Disk encryption and system passwords are enabled across organization workstations.	Inspected the disk encryption configuration and password enforcement configuration to determine that disk encryption and system passwords were enabled across organization workstations.	No exceptions noted.
CC6.7.4	A mobile device management (MDM) system is in place to centrally manage mobile devices supporting the service.	Inspected the MDM system configurations and acceptable use standard to determine that a MDM system was in place to centrally manage mobile devices supporting the service.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.7.5	The organization uses its cloud provider key management service to encrypt data at rest and to store and manage encryption keys. Access to production access keys is restricted to authorized individuals.	Inspected database encryption configuration to determine that the organization used its cloud provider key management service to encrypt data at rest and to store and manage encryption keys.	No exceptions noted.
		Inspected the listing of users with access to production access keys to determine that access to production access keys was restricted to authorized individuals.	No exceptions noted.
CC6.7.6	Customer credentials for integrations are stored in encrypted format and access to the customer credentials is restricted.	Inspected the customer authentication system and a list of users with access to customer credentials to verify that client credentials for integrations were store in an encrypted format and access to customer credentials was restricted to personnel with production system access.	No exceptions noted.
CC6.8 – The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC6.8.1	Security software (firewall, anti-virus, and anti-spam) is installed and enabled on workstations.	Inspected the endpoint security report and Windows firewall to determine that security software was installed and enabled on workstations.	No exceptions noted.
CC6.8.2	The IDS tool is configured to prevent the use of removable media devices on registered endpoints.	Inspected the IDS configurations to determine that the IDS tool was configured to prevent the use of removable media devices on registered endpoints.	No exceptions noted.
CC6.8.3	Infrastructure supporting the service is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the patch management process to determine that infrastructure supporting the service was patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service were hardened against security threats.	No exceptions noted.
System Operations			
CC7.1 – To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
CC7.1.1	The IDS tool is configured to prevent the use of removable media devices on registered endpoints.	Inspected the IDS configurations to determine that the IDS tool was configured to prevent the use of removable media devices on registered endpoints.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.1.2	Logging is enabled to monitor activities such as administrative activities, logon attempts, changes to functions, security configurations, permissions, and roles. Automated alerts are configured to notify IT management and issues identified are resolved in a timely manner through the incident management process.	Inspected the logging, monitoring, and alerting configurations to determine that logging was enabled to monitor administrative activities, logon attempts, changes to functions, security configurations, permissions, and roles.	No exceptions noted.
		Inspected an example alert to determine that automated alerts were configured to notify IT management and issues identified were resolved in a timely manner through the incident management process.	No exceptions noted.
CC7.1.3	Enterprise monitoring tools are configured to monitor system capacity and availability issues and alert cloud operations personnel when pre-defined thresholds are met. System changes are implemented as needed to help ensure that processing capacity can meet demand.	Inspected the monitoring configuration alarm settings and an example alert notification to determine that enterprise monitoring tools were configured to monitor system capacity and availability issues and alert cloud operations personnel when pre-defined thresholds were met.	No exceptions noted.
		Inspected the auto scale configuration to determine that system changes were implemented as needed to help ensure that processing capacity can meet demand.	No exceptions noted.
CC7.1.4	A third-party penetration test is performed on an annual basis to identify vulnerabilities and deficiencies. Remediation plans are proposed and monitored through resolution.	Inspected the penetration test to determine that a third-party penetration test was performed during the period to identify vulnerabilities and deficiencies.	No exceptions noted.
CC7.1.5	Vulnerability scans are performed on a daily basis to identify threats and vulnerabilities to the production systems. Issues identified are analyzed and remediated in a timely manner.	Inspected the vulnerability dashboard and configuration to determine that vulnerability scans were performed on a daily basis to identify threats and vulnerabilities to the production systems.	No exceptions noted.
		Inspected an example remediation ticket to determine that issues identified were analyzed and remediated in a timely manner.	No exceptions noted.

Control #	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.			
CC7.2.1	Security incident response policies and procedures are documented and provide guidance to Company personnel for detecting, responding to, and recovering from security events and incidents.	Inspected the incident response policies and procedures to determine that security incident response policies and procedures were documented and provided guidance to company personnel for detecting, responding to, and recovering from security events and incidents.	No exceptions noted.
CC7.2.2	Incidents related to security, availability, and confidentiality are logged, tracked, and communicated to affected parties (where applicable) by management until resolved. Incidents are evaluated to determine whether they could have resulted in a failure to meet security, availability, and confidentiality commitments and objectives.	Inspected the incident ticket and communication documentation for a listing of incidents reported during the period to determine that for each incident sampled, incidents were logged, tracked, and communicated to affected parties by management until resolved and that incidents were evaluated to determine whether they could have resulted in a failure to meet security, availability, and confidentiality commitments and objectives.	No exceptions noted.
CC7.3 – The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.3.1	Security incident response policies and procedures are documented and provide guidance to Company personnel for detecting, responding to, and recovering from security events and incidents.	Inspected the incident response policies and procedures to determine that security incident response policies and procedures were documented and provided guidance to company personnel for detecting, responding to, and recovering from security events and incidents.	No exceptions noted.
CC7.3.2	Incidents related to security, availability, and confidentiality are logged, tracked, and communicated to affected parties (where applicable) by management until resolved. Incidents are evaluated to determine whether they could have resulted in a failure to meet security, availability, and confidentiality commitments and objectives.	Inspected the incident ticket and communication documentation for a listing of incidents reported during the period to determine that for each incident sampled, incidents were logged, tracked, and communicated to affected parties by management until resolved and that incidents were evaluated to determine whether they could have resulted in a failure to meet security, availability, and confidentiality commitments and objectives.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.4 - The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.4.1	Security incident response policies and procedures are documented and provide guidance to Company personnel for detecting, responding to, and recovering from security events and incidents.	Inspected the incident response policies and procedures to determine that security incident response policies and procedures were documented and provided guidance to company personnel for detecting, responding to, and recovering from security events and incidents.	No exceptions noted.
CC7.4.2	Incidents related to security, availability, and confidentiality are logged, tracked, and communicated to affected parties (where applicable) by management until resolved. Incidents are evaluated to determine whether they could have resulted in a failure to meet security, availability, and confidentiality commitments and objectives.	Inspected the incident ticket and communication documentation for a listing of incidents reported during the period to determine that for each incident sampled, incidents were logged, tracked, and communicated to affected parties by management until resolved and that incidents were evaluated to determine whether they could have resulted in a failure to meet security, availability, and confidentiality commitments and objectives.	No exceptions noted.
CC7.4.3	The organization documents its breach assessment and notification process in the event of a breach.	Inspected the incident management policy to determine that the organization documented its breach assessment and notification process in the event of a breach.	No exceptions noted.
CC7.5 – The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	Security incident response policies and procedures are documented and provide guidance to Company personnel for detecting, responding to, and recovering from security events and incidents.	Inspected the incident response policies and procedures to determine that security incident response policies and procedures were documented and provided guidance to company personnel for detecting, responding to, and recovering from security events and incidents.	No exceptions noted.
CC7.5.2	Incidents related to security, availability, and confidentiality are logged, tracked, and communicated to affected parties (where applicable) by management until resolved. Incidents are evaluated to determine whether they could have resulted in a failure to meet security, availability, and confidentiality commitments and objectives.	Inspected the incident ticket and communication documentation for a listing of incidents reported during the period to determine that for each incident sampled, incidents were logged, tracked, and communicated to affected parties by management until resolved and that incidents were evaluated to determine whether they could have resulted in a failure to meet security, availability, and confidentiality commitments and objectives.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.5.3	The organization documents its breach assessment and notification process in the event of a breach.	Inspected the incident management policy to determine that the organization documented its breach assessment and notification process in the event of a breach.	No exceptions noted.
CC.7.5.4	An information security incident tabletop exercise is performed on an annual basis to test the incident response plan.	Inspected the most recent incident response test results to determine that an annual information security incident tabletop exercise was performed to test the information security incident response plan during the period.	No exceptions noted.
Change Management			
CC8.1 – The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC8.1.1	The organization has a documented change management policy made available to personnel that communicates the process for managing changes to the environment.	Inspected the change management policy to determine that the organization had a documented change management policy made available to personnel that communicated the process for managing changes to the environment.	No exceptions noted.
CC8.1.2	A formal SDLC methodology is in place that governs the project planning, design, acquisition, testing, implementation, maintenance, and decommissioning of information systems and related technologies.	Inspected the system acquisition, development, and maintenance procedure document to determine that a formal SDLC methodology was in place that governed the project planning, design, acquisition, testing, implementation, maintenance, and decommissioning of information systems and related technologies.	No exceptions noted.
CC8.1.3	Changes to the application(s) and supporting infrastructure are documented, tested, and approved by authorized personnel prior to implementation into the production environment in accordance with the change management process.	Inspected the change management policy and the change tickets for a sample of application and infrastructure changes implemented during the period to determine that changes to the applications were documented, tested, and approved by authorized personnel prior to implementation into the production environment in accordance with the change management policy for each change sampled.	No exceptions noted.
CC8.1.4	Development and testing activities are performed in development and testing environments that are logically separate from the production environment.	Inspected the network segmentation configurations to determine that development and testing activities were performed in development and testing environments that were logically separate from the production environment.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.1.5	Customer production data is not used in testing or development environments.	Inspected the testing and development environment database to determine that customer production data was not used in testing or development environments.	No exceptions noted.
CC8.1.6	Access to promote changes to production is restricted to authorized personnel based on job responsibilities.	Inspected the list of users with access to promote changes to the production environment to determine that the ability the promote changes into the production environment was restricted to authorized personnel with relevant job responsibilities.	No exceptions noted.
CC8.1.7	Release notes for changes that affect the system are documented and communicated to internal and external users.	Inspected the release notes webpage to determine that release notes for changes that affected the system were documented and communicated to internal and external users.	No exceptions noted.
CC8.1.8	Emergency change requests are documented and subject to the standard change management process but at an accelerated timeline. Prior to initiating an emergency change, appropriate approval is obtained and documented.	Inspected the change management policy and the change tickets for a sample of emergency changes throughout the period to verify that emergency changes were documented, approved, and were released at an accelerated timeline.	No exceptions noted.
CC8.1.9	Documented integration policies and procedures have been established to provide guidelines for managing system integrations.	Inspected the data integrity policies to determine that documented integration policy and procedures have been established to provide guidelines for managing system integrations.	No exceptions noted.
CC8.1.10	Access to make changes to Integrations is restricted to authorized individuals.	Inspected the list of users with access to make changes to integrations to determine that the ability to make changes to integrations was restricted to authorized personnel with relevant job responsibilities.	No exceptions noted.
CC8.1.11	An incident management process is invoked for timely resolution of identified data integration errors in accordance with the system commitments.	Inspected the tickets for a sample of errors detected during the period to determine that an incident management process was invoked for timely resolution of identified data integration errors in accordance with the system commitments.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.1.12	Changes to integrations are documented, tested, and approved by authorized personnel prior to implementation into the production environment in accordance with the change management process.	Inspected the change tickets for a sample of integration changes during the period to determine that changes to integrations were documented, tested, and approved by authorized personnel prior to implementation into the production environment in accordance with the change management process.	No exceptions noted.
CC8.1.13	Logging is enabled to monitor activities such as administrative activities, logon attempts, changes to functions, security configurations, permissions, and roles. Automated alerts are configured to notify IT management and issues identified are resolved in a timely manner through the incident management process.	Inspected the logging, monitoring, and alerting configurations to determine that logging was enabled to monitor administrative activities, logon attempts, changes to functions, security configurations, permissions, and roles.	No exceptions noted.
		Inspected an example alert to determine that automated alerts were configured to notify IT management and issues identified were resolved in a timely manner through the incident management process.	No exceptions noted.
CC8.1.14	Users do not have the ability to modify auto evidence collection output data.	Inspected the auto evidence collection configuration to determine that users did not have the ability to modify auto evidence collection output data.	No exceptions noted.
Risk Mitigation			
CC9.1 – The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	A documented risk methodology program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk methodology document to determine that a documented risk management program was in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks	No exceptions noted.
CC9.1.2	A formal risk assessment process is performed on at least an annual basis. Risks that are identified are rated using a risk evaluation process and are formally documented, with mitigation strategies for management review.	Inspected the documentation for the most recently completed risk assessment to determine that a risk assessment was performed during the period and that identified risks were rated using a risk evaluation process and were formally documented, with mitigation strategies for management review.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.1.3	Management maintains insurance coverage through an external service provider against major financial risks and cyber risks for the overall business.	Inspected the cyber security insurance policy to determine that management maintained insurance coverage through an external service provider against financial and cyber risks for the overall business.	No exceptions noted.
CC9.1.4	A disaster recovery plan is in place to guide personnel in procedures against disruptions caused by an unexpected event. The plan is tested at least annually.	Inspected the disaster recovery plan and completed disaster recovery test results to determine that a disaster recovery plan was in place to guide personnel in procedures to protect against disruptions caused by an unexpected event and that the plan was tested during the period.	No exceptions noted.
CC9.2 – The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	Formal policies and procedures that outline the requirements for vendor management are documented and include the following components: • Maintaining a list of critical vendors • Requirements for the assessment of risks resulting from the procurement of third-party services • Requirements for the classification of third parties • Information security requirements for the processing, storage, or transmission of information by third parties • Specifications for the contractual agreement and monitoring of third-party vendor requirements • Requirements for critical vendors to maintain their own security practices and procedures • Annually reviewing attestation reports for critical vendors or performing a vendor risk assessment	Inspected the vendor management policies and procedures to determine that formal policies and procedures that outlined the requirements for vendor management were documented and included the following components: • Maintaining a list of critical vendors • Requirements for the assessment of risks resulting from the procurement of third-party services • Requirements for the classification of third parties • Information security requirements for the processing, storage, or transmission of information by third parties • Specifications for the contractual agreement and monitoring of third-party vendor requirements • Requirements for critical vendors to maintain their own security practices and procedures • Annually reviewing attestation reports for critical vendors or performing a vendor risk assessment	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.2.2	Management obtains and reviews the subservice organizations third-party compliance reports on an annual basis.	Inspected the attestation reports and the completed risk assessments for a sample of critical vendors engaged with throughout the period to determine that management obtained and reviewed the subservice organization's third-party compliance reports during the period.	No exceptions noted.
CC9.2.3	A vendor risk assessment is performed at least annually for critical vendors. Exceptions noted in the vendor risk assessments are evaluated to determine impact on service.	Inspected the vendor risk assessment for a sample of critical vendors to determine that a vendor risk assessment is performed at annually for critical vendors and that exceptions noted in the vendor risk assessments are evaluated to determine impact on service.	No exceptions noted.

Additional Criteria for Availability

Control #	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.			
A1.1.1	The organization utilizes OneTrust platform to manage its Information Security policies and procedures. Internal policy and procedure documents relating to security, confidentiality, and availability are maintained and made available to employees. The policies and procedure documents are reviewed and approved by management annually or during significant changes.	Inspected the information security policies and procedures shared on the OneTrust platform to determine that the Company utilized the OneTrust platform to manage its information security policies and procedures related to security, confidentiality, and availability and were maintained and made available to employees.	No exceptions noted.
		Inspected the information security policies on the company intranet to determine that documents were reviewed and approved by management annually or during significant changes.	No exceptions noted.
A1.1.2	Enterprise monitoring tools are configured to monitor system capacity and availability issues and alert cloud operations personnel when pre-defined thresholds are met. System changes are implemented as needed to help ensure that processing capacity can meet demand.	Inspected the monitoring configuration alarm settings and an example alert notification to determine that enterprise monitoring tools were configured to monitor system capacity and availability issues and alert cloud operations personnel when pre-defined thresholds were met.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the auto scale configuration to determine that system changes were implemented as needed to help ensure that processing capacity can meet demand.	No exceptions noted.
A1.1.3	Future processing demand is forecasted and compared to schedule capacity on an ongoing basis. Forecasts are reviewed and approved by IT management. Change requests are initiated as needed based on approved forecasts.	Inspected the capacity monitoring and forecast report and approval from management to verify that future processing demand was forecasted and scheduled to ensure that processing demand was met and forecasts were approved by management.	No exceptions noted.
A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.			
A1.2.1	Documented procedures outline the process the Company's staff follows to back up and recover customer data. The procedures are reviewed by management at least annually.	"Inspected the backup and restoration policy document to determine that documented procedures outlined the process that the Company's staff followed to back up and recover customer data and that the document was reviewed by management annually.	No exceptions noted.
A1.2.2	Daily incremental back-ups are performed using an automated system and replicated to an offsite location.	Inspected the backup configuration to determine that daily incremental back-ups are performed and replicated to an offsite location.	No exceptions noted.
A1.2.3	A multi-location strategy is employed for production environments to permit the resumption of operations at other availability zones in the event of the loss of a facility.	Inspected the replication settings for the only database utilized throughout the period to verify that multiple availability zones were utilized to ensure system recoverability through database redundancy through different physical locations.	No exceptions noted.
A1.2.4	A disaster recovery plan is in place to guide personnel in procedures against disruptions caused by an unexpected event. The plan is tested at least annually.	Inspected the disaster recovery plan and completed disaster recovery test results to determine that a disaster recovery plan was in place to guide personnel in procedures to protect against disruptions caused by an unexpected event and that the plan was tested during the period.	No exceptions noted.
CSOC3	AWS is expected to implement control activities that ensure environmental protection controls are in place at facilities housing production infrastructure and backup media where in-scope systems reside.		

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A1.3.1	Backup restoration testing is performed on an annual basis to test the integrity and completeness of back-up information. The incident management process is invoked for anomalies.	Inspected the backup restoration testing to determine that the backup restoration testing was performed on an annual basis to test the integrity and completeness of back-up information and the incident management process was invoked for anomalies.	No exceptions noted.
A1.3.2	Backup restoration testing is performed on an annual basis to test the integrity and completeness of back-up information. The incident management process is invoked for anomalies.	Inspected the backup restoration testing to determine that the backup restoration testing was performed on an annual basis to test the integrity and completeness of back-up information and the incident management process was invoked for anomalies.	No exceptions noted.

Additional Criteria for Confidentiality

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.1 - The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
C1.1.1	The organization utilizes OneTrust platform to manage its Information Security policies and procedures. Internal policy and procedure documents relating to security, confidentiality, and availability are maintained and made available to employees. The policies and procedure documents are reviewed and approved by management annually or during significant changes.	Inspected the information security policies and procedures shared on the OneTrust platform to determine that the Company utilized the OneTrust platform to manage its information security policies and procedures related to security, confidentiality, and availability and were maintained and made available to employees.	No exceptions noted.
		Inspected the information security policies on the company intranet to determine that documents were reviewed and approved by management annually or during significant changes.	No exceptions noted.
C1.1.2	A data classification policy is documented to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the asset management policy to determine that the organization had policies and procedures in place for identification handling and labeling of confidential information related to the sensitivity of the information.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.1.3	Formal data retention and disposal procedures are documented to guide the secure retention and disposal of Company and customer data.	Inspected the asset management policy to determine that formal data retention and disposal procedures were documented to guide the secure retention and disposal of Company and customer data.	No exceptions noted.
C1.1.4	Employees are required to sign a confidentiality agreement upon hire. This agreement prohibits any disclosure of information and other data to which the employee has been granted access during employment and after termination.	Inquired of the senior information security GRC analyst regarding confidentiality agreements to determine that employees are required to sign a confidentiality agreement upon hire and that this agreement prohibits any disclosure of information and other data to which the employee has been granted access during employment and after termination.	No exceptions noted.
		Inspected the listing of employees hired during the period and the query used to generate the listing and determined that no employees were hired during the period; therefore, no testing of operating effectiveness was performed.	
C1.2 - The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			
C1.2.1	The organization utilizes OneTrust platform to manage its Information Security policies and procedures. Internal policy and procedure documents relating to security, confidentiality, and availability are maintained and made available to employees. The policies and procedure documents are reviewed and approved by management annually or during significant changes.	Inspected the information security policies and procedures shared on the OneTrust platform to determine that the Company utilized the OneTrust platform to manage its information security policies and procedures related to security, confidentiality, and availability and were maintained and made available to employees.	No exceptions noted.
		Inspected the information security policies on the company intranet to determine that documents were reviewed and approved by management annually or during significant changes.	No exceptions noted.
C1.2.2	A data classification policy is documented to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the asset management policy to determine that the organization had policies and procedures in place for identification handling and labeling of confidential information related to the sensitivity of the information.	No exceptions noted.
C1.2.3	Formal data retention and disposal procedures are documented to guide the secure retention and disposal of Company and customer data.	Inspected the asset management policy to determine that formal data retention and disposal procedures were documented to guide the secure retention and disposal of Company and customer data.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.2.4	Electronic media containing confidential information is purged or destroyed, and certificates of destruction are issued for each device destroyed.	Inspected the certificate of destruction for a sample of disposed assets throughout the period to verify data and software stored on equipment was confirmed to removed and rendered unreadable prior to disposal.	No exceptions noted.