

OneNotary

ONENOTARY, INC.

SOC 2 REPORT

FOR

ONENOTARY PLATFORM

A TYPE 2 INDEPENDENT SERVICE AUDITOR'S
REPORT ON CONTROLS RELEVANT TO SECURITY

NOVEMBER 1, 2023, TO FEBRUARY 29, 2024

Attestation and Compliance Services



Proprietary & Confidential

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

This report is intended solely for use by the management of OneNotary, Inc., user entities of OneNotary, Inc.'s services, and other parties who have sufficient knowledge and understanding of OneNotary, Inc.'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 1 INDEPENDENT SERVICE AUDITOR'S REPORT	1
SECTION 2 MANAGEMENT'S ASSERTION	5
SECTION 3 DESCRIPTION OF THE SYSTEM	7
SECTION 4 TESTING MATRICES	23

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To OneNotary, Inc.:

Scope

We have examined OneNotary, Inc.'s ("OneNotary" or the "service organization") accompanying description of its OneNotary Platform system, in Section 3, throughout the period November 1, 2023, to February 29, 2024, (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 November 1, 2023, to February 29, 2024, to provide reasonable assurance that OneNotary's service commitments and system requirements were achieved based on the trust services criteria relevant to security ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

OneNotary uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at OneNotary, to achieve OneNotary's service commitments and system requirements based on the applicable trust services criteria. The description presents OneNotary's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of OneNotary'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

OneNotary 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 OneNotary's service commitments and system requirements were achieved. OneNotary has provided the accompanying assertion, in Section 2, ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. OneNotary 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). 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

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

Inherent Limitations

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

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

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

Description of 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:

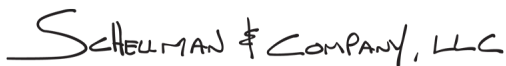
- a. the description presents OneNotary's Platform system that was designed and implemented throughout the period November 1, 2023, to February 29, 2024, in accordance with the description criteria;
- b. the controls stated in the description were suitably designed throughout the period November 1, 2023, to February 29, 2024, to provide reasonable assurance that OneNotary'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 OneNotary's controls throughout that period; and
- c. the controls stated in the description operated effectively throughout the period November 1, 2023, to February 29, 2024, to provide reasonable assurance that OneNotary'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 OneNotary'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 OneNotary; user entities of OneNotary's Platform system during some or all of the period of November 1, 2023, to February 29, 2024, business partners of OneNotary subject to risks arising from interactions with the OneNotary Platform 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.

SCHEFFMAN & COMPANY, LLC

Tampa, Florida
March 19, 2024

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We have prepared the accompanying description of OneNotary's Platform system, in Section 3, throughout the period November 1, 2023, to February 29, 2024, (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 OneNotary Platform system that may be useful when assessing the risks arising from interactions with OneNotary's system, particularly information about system controls that OneNotary has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

OneNotary uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at OneNotary, to achieve OneNotary's service commitments and system requirements based on the applicable trust services criteria. The description presents OneNotary's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of OneNotary'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:

- a. the description presents OneNotary's Platform system that was designed and implemented throughout the period November 1, 2023, to February 29, 2024, in accordance with the description criteria;
- b. the controls stated in the description were suitably designed throughout the period November 1, 2023, to February 29, 2024, to provide reasonable assurance that OneNotary's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations applied the complementary controls assumed in the design of OneNotary's controls throughout that period; and
- c. the controls stated in the description operated effectively throughout the period November 1, 2023, to February 29, 2024, to provide reasonable assurance that OneNotary'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 OneNotary's controls operated effectively throughout that period.

SECTION 3

DESCRIPTION OF THE SYSTEM

OVERVIEW OF OPERATIONS

Company Background

OneNotary is a San Francisco-based online notarization platform founded in 2020. It is focused on providing a secure and efficient remote online notarization solution for individuals and businesses nationwide.

Description of Services Provided

OneNotary is a legal, fast, and secure online notary service available 24x7. It covers unique client requests and provides:

- witness provision;
- multi-language notary;
- ability to perform simultaneous sessions with up to five participants in different locations; and
- notarization from a specific state (some documents require a notary only from their own state).

The OneNotary Platform programming interface (API) provides the ability to have advanced white-label integration within hours.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Principal Service Commitments

OneNotary designs its processes and procedures related to the OneNotary platform to meet its objectives for its OneNotary platform services. Those objectives are based on the principal service commitments that OneNotary makes to user entities, the laws and regulations that govern the provision of the OneNotary platform, and the financial, operational, and compliance requirements that OneNotary has established for the services. The OneNotary platform is subject to the relevant regulatory and industry information and data security requirements in which OneNotary operates.

Security commitments to user entities are documented and communicated in the terms of service, as well as in the description of the service offering provided on the OneNotary company website.

The principal security commitments are standardized and include the following:

- Maintain reasonable physical and technical safeguards to prevent unauthorized disclosure of or access to user data, in accordance with industry standards
- Take reasonable steps to protect the confidential information
- Implement technical and organizational security measures to protect against the loss, misuse, and/or alteration of data

System Requirements

OneNotary has put into place a set of system requirements including policies and procedures to help ensure that principal service commitments are met. Information security policies and procedures define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired, trained, and managed. In addition to these policies, procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the service

provided. Management has identified actions, in the form of control activities, and put into place policies and procedures to enforce those standards.

In accordance with management’s assertion, and the description criteria, the aforementioned principal 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 principal service commitments and requirements made to 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

The production information systems are located at facilities hosted by Amazon Web Services (AWS). OneNotary does not own or maintain the hardware located in AWS data centers and operates under a shared security responsibility model. AWS is responsible for the security of the underlying cloud infrastructure (e.g., physical infrastructure, geographical regions, availability zones, edge locations), and OneNotary is responsible for securing the platform deployed in AWS (e.g., customer data, applications, identity access management, operating system and network firewall configuration, network traffic, server-side encryption).

The in-scope infrastructure consists of multiple applications, operating system platforms, and databases, as shown in the table below:

Primary Infrastructure			
Production System	Business Function Description	Operating System Platform	Physical Location
Google Workspace	Vendor-provided secure identity management.	Google	Google
Virtual private network (VPN)	Encrypted VPN utilized for back-end access to the production environment.	Tunnelblick	AWS
Bastion Host	Authentication gateway that restricts access to the production servers once authenticated to the production VPN.	Amazon Linux	
Amazon Elastic Container Service (ECS)	Managed container orchestration service used to deploy, manage, and scale containerized applications.	Amazon ECS	
AWS Fargate	Serverless compute engine used with Amazon ECS to run containers.	Amazon Linux	
Amazon Elastic Compute Cloud (EC2)	Production server operating systems hosting various specialized services supporting the main application.	Amazon Linux Ubuntu	

Primary Infrastructure			
Production System	Business Function Description	Operating System Platform	Physical Location
Amazon Relational Database Service (RDS)	Database solution for storage of operational data.	PostgreSQL	AWS

In addition, OneNotary utilizes the following systems to support the OneNotary platform:

- Amazon Simple Storage Service (S3) – object storage service utilized for secure attachment storage for OneNotary.
- Amazon GuardDuty – monitoring utility utilized to monitor the production environment for suspicious or anomalous activity and alert engineering personnel when predefined thresholds are met or exceeded.
- Amazon CloudWatch – application and infrastructure monitoring tool utilized to collect monitoring and operational data (logs, metrics, and events) and is used to detect anomalous behavior, set alarms, visualize logs, and metrics.
- AWS CloudTrail – web service utilized to record and log AWS API call information, including: API caller, time, source Internet protocol (IP) address request parameters, and response elements.
- AWS Key Management Service (KMS) – managed service utilized to create and control encryption keys used to encrypt data used by OneNotary in AWS.
- GitLab – version control software utilized to control access to source code and provide roll back capabilities for application changes.
- Bandit – security scanning software utilized to conduct vulnerability scans of application source code.
- Safety – security scanning software utilized to conduct dependency vulnerability scans of application source code.
- Jamf – mobile device management (MDM) tool utilized to manage and enforce security requirements on OneNotary-owned workstations.
- Notion – productivity and note-taking application utilized for task management and project tracking.
- AWS Lambda – serverless compute service utilized to run code without having to provision or manage servers.
- Amazon Simple Notification Service (SNS) – web service utilized to coordinate and manage the delivery or sending of messages to subscribing endpoints or clients.
- Slack – communications platform utilized to facilitate daily conversations related to various aspects of the business.

People

OneNotary provides support for the above services in each of the following functional areas:

- Management – responsible for company-wide strategy, goals, resources, and risk management.
- Research and development (R&D) – responsible for innovating and improving the technology and services through enhancements of the platform, development of new features, and helping to ensure security and reliability.
- Operations and sales – responsible for the day-to-day operations of the organization, helping to ensure its smooth functioning and management of notaries. This team also focuses on activities to attract clients, close deals, and nurture client relationships to drive business growth.

- In-house notaries – responsible for performing notarial acts, including verifying signers' identities, witnessing document signings, and applying notarial seals or stamps. The in-house notaries also guide clients through the notarization process and maintain accurate records.
- Implementation and support – responsible for the setup of the organization's services for clients, while offer ongoing support. This team also helps clients transition smoothly to the platform, provide technical and operational assistance, and address customer inquiries and concerns.

Procedures

Access, Authentication, and Authorization

The engineering team has formally documented standard build procedures for installation and maintenance of production servers that includes the requirement for access control systems to enforce logical access. Access to production resources is controlled using permissions associated with OneNotary staff and controlled system accounts. The in-scope systems (e.g., Google, bastion host, servers, databases, AWS management console, VPN, etc.) are configured to authenticate users with a user account and minimum password requirements or secure shell (SSH) public key authentication, and to enforce multi-factor authentication (MFA) as applicable. Predefined security groups are utilized to assign role-based access privileges and restrict access to date to the in-scope systems.

The production network is segmented to help ensure that confidential data is isolated from other unrelated networks. To access production servers and databases from the back-end, users must first authenticate to the production environment through an encrypted VPN, secured with advanced encryption standard-256 (AES-256) encryption. Users are authenticated with a user-specific certificate before establishing a VPN session. Once connected to the production VPN, users must then authenticate to a bastion host via SSH. Once connected to the bastion host, users may authenticate to the production servers via SSH. Access to the production databases requires the users to be authenticated to the underlying database server via the aforementioned server authentication process. Further, to access the production environment from the front-end via the AWS console, users authenticate to the AWS console via username, password, and MFA.

Administrator access to the production systems is granted based on job roles and responsibilities and limited to authorized personnel. Further, the ability to install applications or software is restricted to authorized engineering personnel. To help ensure access privileges are appropriate, access reviews including privileged users are performed on a quarterly basis to help ensure that access to the in-scope systems is restricted to authorized employees.

Access Requests and Access Revocation

Management has established controls to help ensure that access to data is restricted to those who require access. When a new employee is hired and has accepted a position at OneNotary, user access provisioning and onboarding requirements are documented as part of a new hire checklist. Employee access requests are documented in an access request task and require the approval of management prior to access being granted.

Upon notification of an employee termination from the employee's manager, HR or operations personnel initiate a communication to system owners to help ensure that employees do not retain system access subsequent to their termination date. HR or operations personnel, in collaboration with other system owners, will disable the employee's system access.

Network Security and Endpoint Management

An intrusion detection system (IDS) is configured to report network events related to suspected or actual unauthorized access from outside the system boundaries.

AWS security groups are configured to prevent unauthorized access from sources outside system boundaries. An automated monitoring tool is configured to monitor AWS security group changes and send alerts to engineering personnel via the internal collaboration tool upon detected configuration changes. Additionally, security groups are reviewed on a quarterly basis to help ensure that only necessary connections are configured.

Linux-based technology and software architecture is in place which minimizes the risk of production servers being infected by computer viruses, malicious code, and unauthorized software. Additionally, MDM software is configured to install and manage enterprise anti-malware software on OneNotary-owned workstations.

Change Management

OneNotary has a process in place to help provide reasonable assurance that unauthorized changes are not made to production systems. Documented change control policies and procedures are in place to guide personnel in performing changes to production systems.

Engineering team meetings are held on a quarterly basis to discuss and communicate the ongoing and upcoming projects that affect the system.

Development and testing activities are performed in distinct environments that are logically separate from production to help ensure that changes made within the development and staging environments do not affect the production environment. Additionally, customer data is not utilized for application change control development or testing.

A change tracking system is in place to centrally maintain, manage, and monitor application and infrastructure changes from development through implementation. Changes are authorized, peer reviewed, tested, and approved prior to implementation.

GitLab is utilized as the version control software to restrict access to application source code and provide rollback capabilities. Changes to source code result in the creation of a new version of the code and GitLab records the check-in and check-out, along with the user account associated with the activity. Write and administrator access within GitLab is restricted to user accounts accessible by authorized personnel.

GitLab build pipelines are utilized to perform automated testing and scanning of application source code, including: unit testing, static application security scanning, and dependency vulnerability scanning. Additionally, GitLab is configured to enforce code review and approval by at least one individual independent of the individual who initiated the merge request. The aforementioned are validated prior to application source code being merged into the production branch.

For each new task, engineering personnel create a development branch from the production branch. The engineer creates a merge request to push the change into the staging branch. Testing, scanning, and approval validations are performed for each merge request via the aforementioned GitLab build pipelines. The aforementioned process is repeated prior to introducing changes into the production environment, which also requires a new merge request and approval. Approved code changes are deployed to the production environment by authorized engineering personnel via GitLab.

Additionally, OneNotary management monitors for application changes deployed outside of the standard change management process on a daily basis. Exceptions are investigated and logged.

System Monitoring

The engineering team has formally documented standard build procedures for installation and maintenance of production servers.

Vulnerability assessments, including application source code and dependency vulnerability scanning, are performed on at least a monthly basis. Additionally, penetration testing is performed by a third-party vendor on an annual basis. Security vulnerabilities that are identified either via the annual penetration test or monthly vulnerability scans are triaged by the security team and monitored through resolution.

Additionally, the following are in place to report and notify OneNotary personnel of certain system events:

- An IDS is configured to report network events related to suspected or actual unauthorized access from outside the system boundaries.
- Logging and monitoring software is configured to collect data from system infrastructure components and endpoint systems to monitor system performance, potential security vulnerabilities, and resource utilization.
- An automated monitoring tool is configured to monitor AWS security group changes.

Incident Response

Incident response procedures are in place that outline the response procedures to security events and include lessons learned to evaluate the effectiveness of the procedures. Further, the incident response procedures include, but are not limited to, remediation of the incident, restoration of operations, communication protocols and timing to affected parties, and lessons learned. The procedures are reviewed on an annual basis to help ensure they are effectively meeting the business objectives. OneNotary utilizes an internal incident tracking system to document the identification, escalation, and resolution of security incidents. Closed security incidents are reviewed and approved by management to help ensure that the incident response procedures were followed, and that the incident was resolved. Security management meetings are held on a quarterly basis to discuss the effect of identified security vulnerabilities on the ability to meet business objectives and to identify corrective measures. Additionally, engineering personnel complete incident postmortem reports upon system outages that include the incident and impact analysis, resolutions, lessons learned, and action items.

Data

Data within the OneNotary platform is generated and uploaded by OneNotary customers via the web browser or API integrations. Customers have the ability to retrieve reports related to their respective workspaces through the OneNotary platform. If an error is identified, customers contact customer support and provide feedback to correct and resolve the issues. Significant events and conditions are captured in the system and application logs.

OneNotary data is categorized according to the data classification standard and is protected according to its classification. The policy has three categories:

- Confidential – data which is legally regulated.
- Internal – internal data that does not meet the confidential definition.
- Public – data for which there is no expectation for privacy or confidentiality.

Confidential data is stored in an encrypted format utilizing AES-256. Access to manage cryptographic keys is restricted to authorized personnel. Documented policies and procedures are in place that prohibit the transmission of sensitive information over the Internet or other public communications paths unless it is encrypted. The transmission of confidential data is secured via an Internet connection encrypted with the TLS protocol. Additionally, MDM software is configured to encrypt the hard drives of OneNotary-owned workstations.

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	Data Reporting	Classification
User Data	Registration data, including: names, e-mail addresses, and phone numbers.	Confidential
Document Data	Legal documents, contracts, and affidavits.	
Identity Verification Data	IDs used by the signers.	
Notarization Records	Notarization session data, including: details of the documents notarized, ID types, the notary involved, timestamps of the notarization, date and time of the notarial act, type of notarial act, and name of the document.	
Communication Data	Audio and video recordings.	

Data Used and Supported by the System		
Data Description	Data Reporting	Classification
User Preferences and Settings	Notification settings, language preferences, and other user-specific settings.	Confidential
Security and Compliance Data	Access logs, encryption keys, and data related to compliance with relevant notarial laws and regulations.	
R&D and Analytics Data	User feedback, usage patterns, and performance data.	
Notaries Data	Notary commission information and notarial certificates, notary's photo, geographic location, and social media handles.	

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 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 OneNotary, and the types of controls expected to be implemented at AWS to achieve OneNotary's principal service commitments and system requirements based on the applicable trust services criteria.

Control Activities Expected to be Implemented by AWS	Applicable Trust Services Criteria
AWS is responsible for implementing controls to manage logical access to the underlying network, virtualization management software, and storage devices for its cloud hosting services where the OneNotary systems reside.	CC6.1 – CC6.3, CC6.5 – CC6.6
AWS is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.	CC6.4 – CC6.5
AWS is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where the OneNotary systems reside.	CC6.7
AWS is responsible for monitoring the logical access control systems for the underlying network, virtualization management software, and storage devices for its cloud hosting services where the OneNotary systems reside.	CC7.2

CONTROL ENVIRONMENT

The control environment at OneNotary 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 the board of directors.

Integrity and Ethical Values

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

- Management formally documents and reviews the organizational policy statements that communicate entity values and behavioral standards to personnel.
- Employees are required to sign an acknowledgment form upon hire, and on an annual basis thereafter, indicating that they have been given access to the acceptable use policy, which includes standards of employee conduct, and that they understand their responsibility for adhering to the associated policies and procedures.
- Employees are required to sign a confidentiality agreement upon hire agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.
- A background screening is performed for employment candidates as a component of the hiring process.
- An employee sanction policy is in place communicating that an employee may be terminated for noncompliance with a policy and/or procedure.

Executive Management and Board of Directors Oversight

The board of directors oversees the management of OneNotary and delegates the responsibility for day-to-day management to the chief executive officer (CEO) and other senior management. Directors provide the CEO and senior management with guidance and strategic oversight to help build stockholder value. The board of directors' duties and responsibilities include: determining the size and composition of the board of directors; overseeing the management succession process; reviewing and approving strategic and business plans, including financial objectives and budgets; evaluation of the board of directors, individual directors, and board of directors committees; overseeing the financial reporting processes and accounting practices and the assessment of the adequacy and effectiveness of systems of internal controls regarding finance, accounting, and legal and regulatory compliance; assessment and management of major risks; oversight of policies designed to help ensure that the activities of directors and employees are in compliance with legal and ethical conduct standards; and review of governance policies and practices. Specific control activities that OneNotary has implemented in this area are described below:

- The board of directors establishes and maintains a formal charter and set of bylaws which describes their responsibilities and oversight of management's system of internal control.
- The board of directors has sufficient members who are independent from management and are objective in evaluations and decision making.
- Board of directors and committee meetings are held on an annual basis to review internal control performance.

- Management provides internal control performance metrics to the board of directors on an annual basis. These metrics are formally documented in the risk assessment summary for board review.

Organizational Structure and Assignment of Authority and Responsibility

OneNotary's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. OneNotary's management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility and lines of reporting. OneNotary has developed an organizational structure suited to its needs. This organizational structure is based, in part, on its size and the nature of its activities. Specific control activities that OneNotary has implemented in this area are described below:

- The organizational structure, reporting lines, and authorities are defined in organizational charts and communicated to employees via the company intranet.
- Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.
- An executive management team that is comprised of security personnel and executive staff has been established to exercise oversight of the development and performance of internal control.
- Management has assigned the responsibility of the maintenance and enforcement of the entity security policies and procedures to the information security group.

Commitment to Competence

OneNotary management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. OneNotary's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge. Specific control activities that OneNotary has implemented in this area are described below:

- Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.
- New employee hiring procedures are in place to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties as outlined in the job description.
- New employee checklists are completed to guide the hiring process to help ensure that newly hired employees are compliant with the company's employment standards and corporate policies and procedures.
- Employees are required to complete security awareness training upon hire, and on an annual basis thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit security policies.
- Management monitors compliance with security awareness training requirements on an annual basis.
- Performance reviews are conducted on an annual basis to evaluate performance of employees against expected levels of performance.

Accountability

OneNotary's management philosophy and operating style encompasses a broad range of characteristics. Such characteristics may include management's approach to taking and monitoring business risks, management's attitudes and actions toward financial reporting, and management's attitudes toward information processing,

accounting functions and personnel. Specific control activities that OneNotary has implemented in this area are described below:

- Management formally documents and reviews on an annual basis an organization strategy and performance policy to align internal control responsibilities, performance measures, and incentives with company business objectives.
- Management holds a quarterly company-wide strategy meeting that discusses and aligns internal control responsibilities, performance measures, and incentives with company business objectives.
- Management has assigned the responsibility of the maintenance and enforcement of the entity security policies and procedures to the information security group.
- Management provides internal control performance metrics to the board of directors on an annual basis. These metrics are formally documented in the risk assessment summary for board review.
- An employee sanction policy is in place communicating that an employee may be terminated for noncompliance with a policy and/or procedure.
- Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.
- Performance reviews are conducted on an annual basis to evaluate performance of employees against expected levels of performance.

RISK ASSESSMENT

OneNotary has a risk assessment process to identify and manage risks that could affect OneNotary'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, OneNotary has considered the risks that could prevent it from effectively addressing the criteria under the security trust services category.

Objective Setting

Processes and procedures are in place to help ensure that risks are evaluated and that controls are designed, implemented, and operated to address areas, as appropriate, to detect, respond to, mitigate, and recover from security events based on the assessed risks. Areas for evaluation include systems development, computer operations, program changes, and access to programs and data. Implemented controls include preventive and detective controls, such as manual, automated, or information technology (IT)-dependent controls based on the environment in which the entity operates, the nature and scope of the entity's operations, and its specific characteristics. OneNotary 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. OneNotary's risk assessment process includes an analysis of possible threats and vulnerabilities relative to each of the objectives. The risk identification process includes consideration of both internal and external factors and their impact on the achievement of the objectives.

Risk Identification and Analysis

OneNotary 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 OneNotary operates. OneNotary 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.

Identified risks are analyzed through a process that includes estimating the potential significance of the risk. OneNotary's risk assessment process includes considering how the risk should be managed and whether to

accept, avoid, mitigate, or share the risk. OneNotary determines mitigation strategies for the risks that have been identified and designs, develops, and implements controls, including policies and procedures, to implement its risk mitigation strategy.

Risk Factors

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

External Factors

- Technological developments
- Changing customer needs or expectations
- New legislation and regulation that could force changes in policies and strategies
- Natural catastrophes that could lead to changes in operations or information systems
- Economic changes that could have an impact on management decisions

Internal Factors

- Significant changes in policies, processes, or personnel
- Types of fraud, incentives, pressures, opportunities, attitudes, and rationalizations for employees
- A disruption in information systems processing
- The quality of personnel hired, and methods of training utilized
- Changes in management responsibilities

Potential for Fraud

Management considers the potential for fraud when assessing the risks to OneNotary’s objective. The potential for fraud can occur both in financial and non-financial reporting. Management realizes that the potential for fraud can occur when employees are motivated by certain pressures or incentives to commit fraud. The absence of controls, or ineffective controls, provides an opportunity for fraud when combined with an incentive to commit fraud. Therefore, a formal risk assessment is performed on an annual basis that considers the potential for fraud as well as fraud risks introduced from the use of IT and access to information.

Risk Mitigation

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. The program considers the following:

- Compliance objectives
- External laws and regulations
- Tolerance for risk
- Establishment of sub-objectives to support primary objectives
- Potential for fraud
- Third-party vendors that are processing, storing, or transmitting confidential information

Risk assessments are performed by compliance at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed.

Documented policies and procedures are in place to guide personnel in identifying, selecting, and developing risk management strategies specifically addressing the risks arising from potential business disruptions as part of the

risk assessment process. Disaster recovery and business continuity plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event and are reviewed and approved on an annual basis. Business continuity and disaster recovery plans are tested on an annual basis to help ensure the production environment can be recovered in the event of a disaster. The annual risk assessment includes the consideration of business disruptions.

Documented vendor management policies and procedures are in place to guide personnel in assessing and managing risks associated with third parties. OneNotary's vendor and business partner oversight program requires that contracts with vendors or business partners clearly address (a) the size, scope, and nature of services being provided; (b) the hardware, software, and information requirements related to the provision of such services; (c) the responsibilities of each party; (d) the requirements for information security to meet OneNotary's standards; (e) the ability to perform independent audits of the effectiveness of internal control processes; and (f) the requirement to obtain and review a third-party attestation report.

Formal information sharing agreements are in place with critical vendors. These agreements include confidentiality commitments applicable to that entity. Additionally, the security team reviews changes to critical vendors along with their completed on an annual basis to help ensure that third-party vendors are in compliance with the organization's security requirements and to determine the impact of any changes in relation to the organization's objectives and the impact to internal control.

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 category.

Selection and Development of Control Activities

Information security policies and procedures are documented and define the information security rules and requirements for the service environment. These policies and procedures are reviewed by the Security Compliance team at least annually and updated as needed.

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 OneNotary'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 category are applicable to the OneNotary Platform system.

INFORMATION AND COMMUNICATION SYSTEMS

Communication takes such forms as policy, manuals, and electronic communications. Communications also can be made electronically, verbally, and through the actions of management. OneNotary has implemented various methods of communication to help provide assurance that employees understand their individual roles and responsibilities and that significant events are communicated.

Internal Communications

OneNotary has implemented various methods of internally communicating information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control. Specific control activities that OneNotary has implemented in this area are described below:

- Documented policies and procedures are in place to guide personnel with regard to the design, development, implementation, operation, maintenance, and monitoring of in-scope systems. These policies and procedures are communicated to internal personnel via the company intranet.
- Employees are required to sign an acknowledgment form upon hire, and on an annual basis thereafter, indicating that they have been given access to the acceptable use policy, which includes standards of employee conduct, and that they understand their responsibility for adhering to the associated policies and procedures.
- Employees are required to complete security awareness training upon hire, and on an annual basis thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit security policies.
- Management monitors compliance with security awareness training requirements on an annual basis.
- Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.
- Engineering team meetings are held on a quarterly basis to discuss and communicate the ongoing and upcoming projects that affect the system.
- Documented escalation procedures for reporting incidents are provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.
- Management formally documents and reviews on an annual basis an organization strategy and performance policy to align internal control responsibilities, performance measures, and incentives with company business objectives.
- Management holds a quarterly company-wide strategy meeting that discusses and aligns internal control responsibilities, performance measures, and incentives with company business objectives.

External Communications

OneNotary has also implemented various methods of communicating with external parties regarding matters affecting the functioning of internal control. Specific control activities that OneNotary has implemented in this area are described below:

- Information regarding the design and operation of the system and its boundaries is communicated to external users via the company website.
- The entity's security commitments and the associated system requirements, including the security, contractual, and regulatory requirements, are documented in the terms of service.
- The security commitments and obligations of critical vendors are documented and communicated via service agreements or nondisclosure agreements.
- Nondisclosure agreements of confidentiality and protection are required before sharing information designated as confidential with third parties.
- Documented escalation procedures for reporting incidents are provided to external users via the company website to guide users in identifying and reporting failures, incidents, concerns, and other complaints.

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 help ensure the controls are consistently applied as designed.

Ongoing Monitoring

OneNotary utilizes both manual and automated monitoring tools. Management personnel are involved in the day-to-day functioning of each department and provide hands-on training, coaching, and correction. The management team holds meetings on a periodic basis within functional departments to discuss changes to the organization, changes to the production environment, and incidents or events identified by personnel or user entities. Specific control activities that OneNotary has implemented in this area are described below:

- Penetration testing is performed by a third-party vendor on an annual basis. Security vulnerabilities that are identified are triaged by the security team and monitored through resolution.
- Vulnerability assessments are performed on at least a monthly basis. Security vulnerabilities that are identified are triaged by the security team and monitored through resolution.

Separate Evaluations

Evaluation of an entire internal control system may be prompted by a number of reasons. Major strategy or management change, major acquisitions or dispositions, or significant changes in operations or methods of processing information. Evaluations of internal control vary in scope and frequency, depending on the significance of risks being controlled and the importance of the controls in reducing the risks. Controls addressing higher-priority risks and those most essential to reducing a given risk will tend to be evaluated more often.

OneNotary management evaluates the performance of key controls to gain assurance that controls are in place and operating effectively and reviews results of the annual vendor performance assessment. Corrective action is taken as necessary based on the assessment results. Specific control activities that OneNotary has implemented in this area are described below:

- Documented policies and procedures are in place to guide the internal audit function when performing the internal system audit process.
- Internal audits are performed by a third-party on an annual basis. The audit results are documented and reviewed by management.
- Management identifies and assesses changes that could significantly impact the system of internal control during the annual risk assessment process.
- Risk owners perform a review of their assigned controls on an annual basis during the risk assessment process.

Subservice Organization Monitoring

OneNotary obtains and reviews third-party vendor audit reports, such as System and Organization Controls (SOC) reports, on an annual basis to monitor the design and operation effectiveness of the third-party vendor's relevant controls and compliance with security policies. In the event that an issue is identified within a third party's audit report, OneNotary management would determine the necessary actions.

Evaluating and Communicating Deficiencies

Deficiencies in management's internal control system may surface from many sources, including the company's ongoing monitoring procedures, separate evaluations of the internal control system, and external parties. Management has developed protocols to help ensure findings of internal control deficiencies are reported. These

protocols include reporting findings not only to the individual responsible for the function or activity involved, who is in the position to take corrective action, but also to at least one level of management directly above the responsible party. This process enables that individual to provide the necessary support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected. Management evaluates the specific facts and circumstances related to deficiencies in internal control procedures and makes the decision for addressing deficiencies based on whether the incident was isolated or requires a change in the company's procedures or personnel. Specific control activities that OneNotary has implemented in this area are described below:

- Internal audits are performed by a third-party on an annual basis. The audit results are documented and reviewed by management.
- Management provides internal control performance metrics to the board of directors on an annual basis. These metrics are formally documented in the risk assessment summary for board review.
- Management identifies and assesses changes that could significantly impact the system of internal control during the annual risk assessment process.

COMPLEMENTARY CONTROLS AT USER ENTITIES

OneNotary'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 OneNotary Platform system provided by OneNotary. The scope of the testing was restricted to the OneNotary Platform system and its boundaries as defined in Section 3. Schellman conducted the examination testing over the period November 1, 2023, to February 29, 2024.

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 principal service commitments and system requirements, 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	Management formally documents and reviews the organizational policy statements that communicate entity values and behavioral standards to personnel.	Inspected the code of conduct and the acceptable use policy to determine that management formally documented and reviewed the organizational policy statements that communicated entity values and behavioral standards to personnel.	No exceptions noted.
CC1.1.2	Employees are required to sign an acknowledgment form upon hire, and on an annual basis thereafter, indicating that they have been given access to the acceptable use policy, which includes standards of employee conduct, and that they understand their responsibility for adhering to the associated policies and procedures.	Inquired of the compliance consultant regarding the employee acknowledgment to determine that employees completed an acknowledgment form upon hire indicating that they had been given access to the acceptable use policy.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the security awareness training material and completion documentation for a sample of employees hired during the period to determine that each employee sampled signed an acknowledgment form upon hire indicating that they had been given access to the employee handbook, which included standards of employee conduct, and they understood their responsibility for adhering to the associated policies and procedures.	No exceptions noted.
		Inspected the security awareness training material and completion documentation for a sample of current employees to determine that each employee sampled signed an acknowledgment form during the period indicating that they had been given access to the employee handbook, which included standards of employee conduct, and they understood their responsibility for adhering to the associated policies and procedures.	No exceptions noted.
CC1.1.3	Employees are required to sign a confidentiality agreement upon hire agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.	Inspected the signed confidentiality agreement for a sample of employees hired during the period to determine that each employee sampled signed a confidentiality agreement upon hire agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.	No exceptions noted.
CC1.1.4	Background screening is performed for employment candidates as a component of the hiring process.	Inspected the background screening documentation for a sample of employees hired during the period to determine that background screening was performed for employment candidates as a component of the hiring process for each employee sampled.	No exceptions noted.
CC1.1.5	An employee sanction policy is in place communicating that an employee may be terminated for noncompliance with a policy and/or procedure.	Inspected the employee sanction policies and procedures to determine that an employee sanction policy was in place communicating that an employee may be terminated for noncompliance with a policy and/or procedure.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2.1	The board of directors establishes and maintains a formal charter and set of bylaws which describes their responsibilities and oversight of management's system of internal control.	Inspected the board of directors' charter and bylaws to determine that the board of directors established and maintained a formal charter and set of bylaws which described their responsibilities and oversight of management's system of internal control.	No exceptions noted.
CC1.2.2	The board of directors has sufficient members who are independent from management and are objective in evaluations and decision making.	Inspected the listing of board members, the current employee listing, and the organizational chart to determine that the board of directors had sufficient members who were independent from management and were objective in evaluations and decision making.	No exceptions noted.
CC1.2.3	Board of directors and committee meetings are held on an annual basis to review internal control performance.	Inspected the board of directors and committee meeting calendar invitation and the meeting notes to determine that board of directors and committee meetings were held to review internal control performance during the period.	No exceptions noted.
CC1.2.4	Management provides internal control performance metrics to the board of directors on an annual basis. These metrics are formally documented in the risk assessment summary for board review.	Inspected the most recent information security executive team meeting and most recently completed risk assessment to determine that management provided internal control performance metrics to the board of directors and that these metrics were formally documented in the risk assessment summary for board review during the period.	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 organizational structure, reporting lines, and authorities are defined in organizational charts and communicated to employees via the company intranet.	Inspected the organizational chart on the company intranet to determine that the organizational structure, reporting lines, and authorities were defined in organizational charts, and communicated to employees via the company intranet.	No exceptions noted.
CC1.3.2	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the documented position description for a sample of employment positions to determine that documented position descriptions were in place to define the skills, responsibilities, and knowledge levels for particular jobs for each employment position sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.3.3	An executive management team that is comprised of security personnel and executive staff has been established to exercise oversight of the development and performance of internal control.	Inspected the information security policy and the most recent information security executive team meeting calendar invitation and meeting notes to determine that an executive management team that was comprised of security personnel and executive staff had been established to exercise oversight of the development and performance of internal control.	No exceptions noted.
CC1.3.4	Management has assigned the responsibility of the maintenance and enforcement of the entity security policies and procedures to the information security group.	Inspected the information security policy to determine that management had assigned the responsibility of the maintenance and enforcement of the entity security policies and procedures to the information security group.	No exceptions noted.
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the documented position description for a sample of employment positions to determine that documented position descriptions were in place to define the skills, responsibilities, and knowledge levels for particular jobs for each employment position sampled.	No exceptions noted.
CC1.4.2	New employee hiring procedures are in place to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties as outlined in the job description.	Inspected the background screening policy to determine that new employee hiring procedures were in place to guide the hiring process and included verification that candidates possessed the required qualifications to perform the duties as outlined in the job description.	No exceptions noted.
CC1.4.3	New employee checklists are completed to guide the hiring process to help ensure that newly hired employees are compliant with the company's employment standards and corporate policies and procedures.	Inspected the completed new hire checklist for a sample of employees hired during the period to determine that new employee checklists were completed to guide the hiring process to ensure that employees hired during the period were compliant with the company's employment standards and corporate policies and procedures for each employee sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.4.4	Employees are required to complete security awareness training upon hire, and on an annual basis thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	Inspected the security awareness training completion log for a sample of current employees to determine that each employee sampled completed security awareness training to understand their obligations and responsibilities to comply with the corporate and business unit security policies during the period.	No exceptions noted.
		Inspected the security awareness training completion log for a sample of employees hired during the period to determine that each employee sampled completed security awareness training upon hire to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	No exceptions noted.
CC1.4.5	Management monitors compliance with security awareness training requirements on an annual basis.	Inspected the security awareness training completion documentation to determine that management monitored compliance with security awareness training requirements during the period.	No exceptions noted.
CC1.4.6	Performance reviews are conducted on an annual basis to evaluate performance of employees against expected levels of performance.	Inspected the completed performance review for a sample of current employees to determine that performance reviews were conducted to evaluate the performance of employees against expected levels of performance during the period for each employee sampled.	No exceptions noted.
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	Management formally documents and reviews on an annual basis an organization strategy and performance policy to align internal control responsibilities, performance measures, and incentives with company business objectives.	Inspected the information security policy to determine that management formally documented and reviewed an organization strategy and performance policy to align internal control responsibilities, performance measures, and incentives with company business objectives during the period.	No exceptions noted.
CC1.5.2	Management holds a quarterly company-wide strategy meeting that discusses and aligns internal control responsibilities, performance measures, and incentives with company business objectives.	Inquired of the compliance consultant regarding the company-wide strategy meeting to determine that the all-hands meeting was held on a quarterly basis and attendees discussed internal control responsibilities, performance measures and incentives with company business objectives.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the recurring strategy meeting calendar invitation and the meeting slide deck during the period to determine that management held a quarterly company-wide strategy meeting that discussed and aligned internal control responsibilities, performance measures, and incentives with company business objectives for each quarter sampled.	No exceptions noted.
CC1.5.3	Management has assigned the responsibility of the maintenance and enforcement of the entity security policies and procedures to the information security group.	Inspected the information security policy to determine that management had assigned the responsibility of the maintenance and enforcement of the entity security policies and procedures to the information security group.	No exceptions noted.
CC1.5.4	Management provides internal control performance metrics to the board of directors on an annual basis. These metrics are formally documented in the risk assessment summary for board review.	Inspected the most recent information security executive team meeting and most recently completed risk assessment to determine that management provided internal control performance metrics to the board of directors and that these metrics were formally documented in the risk assessment summary for board review during the period.	No exceptions noted.
CC1.5.5	An employee sanction policy is in place communicating that an employee may be terminated for noncompliance with a policy and/or procedure.	Inspected the employee sanction policies and procedures to determine that an employee sanction policy was in place communicating that an employee may be terminated for noncompliance with a policy and/or procedure.	No exceptions noted.
CC1.5.6	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the documented position description for a sample of employment positions to determine that documented position descriptions were in place to define the skills, responsibilities, and knowledge levels for particular jobs for each employment position sampled.	No exceptions noted.
CC1.5.7	Performance reviews are conducted on an annual basis to evaluate performance of employees against expected levels of performance.	Inspected the completed performance review for a sample of current employees to determine that performance reviews were conducted to evaluate the performance of employees against expected levels of performance during the period for each employee sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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	Information system security and data classification and handling policies are formally documented that identify information required to support the functioning of internal control and achievement of objectives and associated protection and access rights.	Inspected the information security and data classification policies and procedures to determine that information system security and data classification and handling policies were formally documented that identified information required to support the functioning of internal control and achievement of objectives and associated protection and access rights.	No exceptions noted.
CC2.1.2	Logging and monitoring software is configured to collect data from system infrastructure components and endpoint systems to monitor system performance, potential security vulnerabilities, and resource utilization, and to alert the engineering team upon detection of unusual system activity or service requests.	Inspected the logging and monitoring software configurations and example alerts generated during the period to determine that logging and monitoring software was configured to collect data from system infrastructure components and endpoint systems to monitor system performance, potential security vulnerabilities, and resource utilization, and to alert the engineering team upon detection of unusual system activity or service requests.	No exceptions noted.
CC2.1.3	Penetration testing is performed by a third-party vendor on an annual basis. Security vulnerabilities that are identified are triaged by the security team and monitored through resolution.	Inspected the most recent penetration testing report and an example vulnerability remediation ticket resolved during the period to determine that penetration testing was performed by a third-party vendor and that security vulnerabilities that were identified were triaged by the security team and monitored through resolution during the period.	No exceptions noted.
CC2.1.4	Vulnerability assessments are performed on at least a monthly basis. Security vulnerabilities that are identified are triaged by the security team and monitored through resolution.	Inquired of the compliance consultant regarding vulnerability assessments to determine that vulnerability assessments were performed on at least a monthly basis and that security vulnerabilities that were identified were triaged by the security team and monitored through resolution.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the vulnerability assessment documentation for a sample of months during the period and an example vulnerability remediation ticket resolved during the period to determine that vulnerability assessments were performed and that security vulnerabilities that were identified were triaged by the security team and monitored through resolution for each month sampled.	No exceptions noted.
CC2.1.5	The entity's IT security group monitors the security impact of emerging technologies and the impact of changes to applicable laws or regulations are considered by senior management.	Inspected evidence of security monitoring during the period to determine that the entity's IT security group monitored the security impact of emerging technologies and the impact of changes to applicable laws or regulations were considered by senior management during the period.	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	Documented policies and procedures are in place to guide personnel with regard to the design, development, implementation, operation, maintenance, and monitoring of in-scope systems. These policies and procedures are communicated to internal personnel via the company intranet.	Inspected the policies and procedures available on the company intranet to determine that documented policies and procedures were in place to guide personnel with regard to the design, development, implementation, operation, maintenance, and monitoring of in-scope systems and that these policies and procedures were communicated to internal personnel via the company intranet.	No exceptions noted.
CC2.2.2	Employees are required to sign an acknowledgment form upon hire, and on an annual basis thereafter, indicating that they have been given access to the acceptable use policy, which includes standards of employee conduct, and that they understand their responsibility for adhering to the associated policies and procedures.	Inquired of the compliance consultant regarding the employee acknowledgment to determine that employees completed an acknowledgment form upon hire indicating that they had been given access to the acceptable use policy.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the security awareness training material and completion documentation for a sample of employees hired during the period to determine that each employee sampled signed an acknowledgment form upon hire indicating that they had been given access to the employee handbook, which included standards of employee conduct, and they understood their responsibility for adhering to the associated policies and procedures.	No exceptions noted.
		Inspected the security awareness training material and completion documentation for a sample of current employees to determine that each employee sampled signed an acknowledgment form during the period indicating that they had been given access to the employee handbook, which included standards of employee conduct, and they understood their responsibility for adhering to the associated policies and procedures.	No exceptions noted.
CC2.2.3	Employees are required to complete security awareness training upon hire, and on an annual basis thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	Inspected the security awareness training completion log for a sample of current employees to determine that each employee sampled completed security awareness training to understand their obligations and responsibilities to comply with the corporate and business unit security policies during the period.	No exceptions noted.
		Inspected the security awareness training completion log for a sample of employees hired during the period to determine that each employee sampled completed security awareness training upon hire to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	No exceptions noted.
CC2.2.4	Management monitors compliance with security awareness training requirements on an annual basis.	Inspected the security awareness training completion documentation to determine that management monitored compliance with security awareness training requirements during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2.5	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the documented position description for a sample of employment positions to determine that documented position descriptions were in place to define the skills, responsibilities, and knowledge levels for particular jobs for each employment position sampled.	No exceptions noted.
CC2.2.6	Engineering team meetings are held on a quarterly basis to discuss and communicate the ongoing and upcoming projects that affect the system.	Inspected the engineering team meeting calendar invitation and meeting minutes for a sample of quarters during the period to determine that engineering team meetings were held for each quarter sampled to discuss and communicate the ongoing and upcoming projects that affect the system.	No exceptions noted.
CC2.2.7	Documented escalation procedures for reporting incidents are provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	Inspected the incident management policies and procedures available to internal users via the company intranet to determine that documented escalation procedures for reporting incidents were provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	No exceptions noted.
CC2.2.8	Management formally documents and reviews on an annual basis an organization strategy and performance policy to align internal control responsibilities, performance measures, and incentives with company business objectives.	Inspected the information security and management policy to determine that management formally documented and reviewed an organization strategy and performance policy to align internal control responsibilities, performance measures, and incentives with company business objectives during the period.	No exceptions noted.
CC2.2.9	Management holds a quarterly company-wide strategy meeting that discusses and aligns internal control responsibilities, performance measures, and incentives with company business objectives.	Inquired of the compliance consultant regarding the company-wide strategy meeting to determine that the all hands meeting was held on a quarterly basis and attendees discussed internal control responsibilities, performance measures and incentives with company business objectives.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the recurring strategy meeting calendar invitation and the meeting slide deck during the period to determine that management held a quarterly company-wide strategy meeting that discussed and aligned internal control responsibilities, performance measures, and incentives with company business objectives for each quarter sampled.	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	Information regarding the design and operation of the system and its boundaries is communicated to external users via the company website.	Inspected the system description on the company website to determine that information regarding the design and operation of the system and its boundaries was communicated to external users via the company website.	No exceptions noted.
CC2.3.2	The entity's security commitments and the associated system requirements, including the security, contractual, and regulatory requirements, are documented in the terms of service.	Inspected the standard customer agreement and an example executed customer agreement to determine that the entity's security commitments and the associated system requirements, including the security, contractual, and regulatory requirements, were documented in the terms of service.	No exceptions noted.
CC2.3.3	The security commitments and obligations of critical vendors are documented and communicated via service agreements or nondisclosure agreements.	Inspected the agreements for a sample of critical vendors to determine that the security commitments and obligations of critical vendors were documented and communicated via service agreements or nondisclosure agreements for each vendor sampled.	No exceptions noted.
CC2.3.4	Nondisclosure agreements of confidentiality and protection are required before sharing information designated as confidential with third parties.	Inspected the nondisclosure agreements for a sample of third-party vendors and the standard customer agreement to determine that nondisclosure agreements of confidentiality and protection were in place before sharing information designated as confidential with third parties for each third party sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.3.5	Documented escalation procedures for reporting incidents are provided to external users via the company website to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	Inspected the company website to determine that documented escalation procedures for reporting incidents were provided to external users via the company website to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	No exceptions noted.
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	Management formally documents an organization strategy and performance policy and updates it on an annual basis to align internal control responsibilities, performance measures, and incentives with company business objectives.	Inspected the information security policy to determine that management formally documented an organization strategy and performance policy and updated it during the period to align internal control responsibilities, performance measures, and incentives with company business objectives.	No exceptions noted.
CC3.1.2	A formal risk assessment is performed on an annual basis that considers risks arising from internal and external factors, including business disruptions, vendors, and the potential for fraud. Risks that are identified are rated using a risk evaluation process that accounts for changes in risk from the prior year, and are formally documented, along with mitigation strategies, for management review.	Inquired of the compliance consultant regarding risks from vendors to determine that a formal risk assessment was performed during the period that considered risks arising from vendors.	No exceptions noted.
		Inspected the most recently completed risk assessment documentation to determine that a formal risk assessment was performed that considered the risks that arise from internal and external factors, including risks arising from potential business disruptions, and the potential for fraud, and that identified risks were rated using a risk evaluation process that accounted for changes in risk from the prior year, and were formally documented, along with mitigation strategies, for management review during the period.	No exceptions noted.
CC3.1.3	Management holds a quarterly company-wide strategy meeting that discusses and aligns internal control responsibilities, performance measures, and incentives with company business objectives.	Inquired of the compliance consultant regarding the company-wide strategy meeting to determine that the all hands meeting was held on a quarterly basis and attendees discussed internal control responsibilities, performance measures and incentives with company business objectives.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the recurring strategy meeting calendar invitation and the meeting slide deck during the period to determine that management held a quarterly company-wide strategy meeting that discussed and aligned internal control responsibilities, performance measures, and incentives with company business objectives for each quarter sampled.	No exceptions noted.
CC3.1.4	Management formally documents and approves risk management policies and procedures to guide personnel in identifying business objective risks, changes to systems, and risk management strategies.	Inspected the risk management policy and procedures to determine that risk management policies and procedures were in place and approved that helped personnel to identify risks, changes to the systems and risk management strategies.	No exceptions noted.
CC3.1.5	Management formally documents and reviews the company's commitments and the operational, reporting, and compliance objectives to help ensure they align with the company's mission and are utilized as part of the annual risk assessment process.	Inspected the most recently completed risk assessment documentation and information security policy to determine that management formally documented and reviewed the company's commitments and the operational, reporting, and compliance objectives to ensure they aligned with the company's mission and were utilized as part of the risk assessment process during the period.	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	Management formally documents and approves risk management policies and procedures to guide personnel in identifying business objective risks, changes to systems, and risk management strategies.	Inspected the risk management policy and procedures to determine that risk management policies and procedures were in place and approved that helped personnel to identify risks, changes to the systems and risk management strategies.	No exceptions noted.
CC3.2.2	A formal risk assessment is performed on an annual basis that considers risks arising from internal and external factors, including business disruptions, vendors, and the potential for fraud. Risks that are identified are rated using a risk evaluation process that accounts for changes in risk from the prior year, and are formally documented, along with mitigation strategies, for management review.	Inquired of the compliance consultant regarding risks from vendors to determine that a formal risk assessment was performed during the period that considered risks arising from vendors.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the most recently completed risk assessment documentation to determine that a formal risk assessment was performed that considered the risks that arise from internal and external factors, including risks arising from potential business disruptions, and the potential for fraud, and that identified risks were rated using a risk evaluation process that accounted for changes in risk from the prior year, and were formally documented, along with mitigation strategies, for management review during the period.	No exceptions noted.
CC3.2.3	Penetration testing is performed by a third-party vendor on an annual basis. Security vulnerabilities that are identified are triaged by the security team and monitored through resolution.	Inspected the most recent penetration testing report and an example vulnerability remediation ticket resolved during the period to determine that penetration testing was performed by a third-party vendor and that security vulnerabilities that were identified were triaged by the security team and monitored through resolution during the period.	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	Management formally documents and approves risk management policies and procedures to guide personnel in identifying business objective risks, changes to systems, and risk management strategies.	Inspected the risk management policy and procedures to determine that risk management policies and procedures were in place and approved that helped personnel to identify risks, changes to the systems and risk management strategies.	No exceptions noted.
CC3.3.2	A formal risk assessment is performed on an annual basis that considers risks arising from internal and external factors, including business disruptions, vendors, and the potential for fraud. Risks that are identified are rated using a risk evaluation process that accounts for changes in risk from the prior year, and are formally documented, along with mitigation strategies, for management review.	Inquired of the compliance consultant regarding risks from vendors to determine that a formal risk assessment was performed during the period that considered risks arising from vendors.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the most recently completed risk assessment documentation to determine that a formal risk assessment was performed that considered the risks that arise from internal and external factors, including risks arising from potential business disruptions, and the potential for fraud, and that identified risks were rated using a risk evaluation process that accounted for changes in risk from the prior year, and were formally documented, along with mitigation strategies, for management review during the period.	No exceptions noted.
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	Management formally documents and approves risk management policies and procedures to guide personnel in identifying business objective risks, changes to systems, and risk management strategies.	Inspected the risk management policy and procedures to determine that risk management policies and procedures were in place and approved that helped personnel to identify risks, changes to the systems and risk management strategies.	No exceptions noted.
CC3.4.2	A formal risk assessment is performed on an annual basis that considers risks arising from internal and external factors, including business disruptions, vendors, and the potential for fraud. Risks that are identified are rated using a risk evaluation process that accounts for changes in risk from the prior year, and are formally documented, along with mitigation strategies, for management review.	<p>Inquired of the compliance consultant regarding risks from vendors to determine that a formal risk assessment was performed during the period that considered risks arising from vendors.</p> <p>Inspected the most recently completed risk assessment documentation to determine that a formal risk assessment was performed that considered the risks that arise from internal and external factors, including risks arising from potential business disruptions, and the potential for fraud, and that identified risks were rated using a risk evaluation process that accounted for changes in risk from the prior year, and were formally documented, along with mitigation strategies, for management review during the period.</p>	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.4.3	The entity's IT security group monitors the security impact of emerging technologies and the impact of changes to applicable laws or regulations are considered by senior management.	Inspected evidence of security monitoring during the period to determine that the entity's IT security group monitored the security impact of emerging technologies and the impact of changes to applicable laws or regulations were considered by senior management during the period.	No exceptions noted.
CC3.4.4	Management obtains and reviews vendor audit reports on an annual basis to help ensure that third-party service providers are in compliance with the organization's requirements.	Inspected the vendor assessment for a sample of critical vendors to determine that management obtained and reviewed vendor audit reports during the period to ensure that third-party service providers were in compliance with the organization's requirements for each third-party sampled.	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	Documented policies and procedures are in place to guide the internal audit function when performing the internal system audit process.	Inspected the internal audit policy and procedures to determine that documented policies and procedures were in place to guide the internal audit function when performing the internal system audit process.	No exceptions noted.
CC4.1.2	Penetration testing is performed by a third-party vendor on an annual basis. Security vulnerabilities that are identified are triaged by the security team and monitored through resolution.	Inspected the most recent penetration testing report and an example vulnerability remediation ticket resolved during the period to determine that penetration testing was performed by a third-party vendor and that security vulnerabilities that were identified were triaged by the security team and monitored through resolution during the period.	No exceptions noted.
CC4.1.3	Vulnerability assessments are performed on at least a monthly basis. Security vulnerabilities that are identified are triaged by the security team and monitored through resolution.	Inquired of the compliance consultant regarding vulnerability assessments to determine that vulnerability assessments were performed on at least a monthly basis and that security vulnerabilities that were identified were triaged by the security team and monitored through resolution.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the vulnerability assessment documentation for a sample of months during the period and an example vulnerability remediation ticket resolved during the period to determine that vulnerability assessments were performed and that security vulnerabilities that were identified were triaged by the security team and monitored through resolution for each month sampled.	No exceptions noted.
CC4.1.4	Internal audits are performed by a third-party on an annual basis. The audit results are documented and reviewed by management.	Inspected the internal audit policies and procedures and the most recently completed internal audit assessment to determine that internal audits were performed by a third-party and that audit results were documented and reviewed by management during the period.	No exceptions noted.
CC4.1.5	Management obtains and reviews vendor audit reports on an annual basis to help ensure that third-party service providers are in compliance with the organization's requirements.	Inspected the vendor assessment for a sample of vendors to determine that management obtained and reviewed vendor audit reports during the period to ensure that third-party service providers were in compliance with the organization's requirements for each third-party sampled.	No exceptions noted.
CC4.1.6	Management identifies and assesses changes that could significantly impact the system of internal control during the annual risk assessment process.	Inspected the most recently completed risk assessment documentation to determine that management identified and assessed changes that could significantly impact the system of internal control as part of the risk assessment process during the period.	No exceptions noted.
CC4.1.7	Risk owners perform a review of their assigned controls on an annual basis during the risk assessment process.	Inspected the most recently completed risk assessment documentation to determine that risk owners performed a review of their assigned controls as part of the risk assessment process during the period.	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	Internal audits are performed by a third-party on an annual basis. The audit results are documented and reviewed by management.	Inspected the internal audit policies and procedures and the most recently completed internal audit assessment to determine that internal audits were performed by a third-party and that audit results were documented and reviewed by management during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.2.2	Management provides internal control performance metrics to the board of directors on an annual basis. These metrics are formally documented in the risk assessment summary for board review.	Inspected the most recent information security executive team meeting and most recently completed risk assessment to determine that management provided internal control performance metrics to the board of directors and that these metrics were formally documented in the risk assessment summary for board review during the period.	No exceptions noted.
CC4.2.3	Management identifies and assesses changes that could significantly impact the system of internal control during the annual risk assessment process.	Inspected the most recently completed risk assessment documentation to determine that management identified and assessed changes that could significantly impact the system of internal control as part of the risk assessment process during the period.	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 formal risk assessment is performed on an annual basis that considers risks arising from internal and external factors, including business disruptions, vendors, and the potential for fraud. Risks that are identified are rated using a risk evaluation process that accounts for changes in risk from the prior year, and are formally documented, along with mitigation strategies, for management review.	Inquired of the compliance consultant regarding risks from vendors to determine that a formal risk assessment was performed during the period that considered risks arising from vendors.	No exceptions noted.
		Inspected the most recently completed risk assessment documentation to determine that a formal risk assessment was performed that considered the risks that arise from internal and external factors, including risks arising from potential business disruptions, and the potential for fraud, and that identified risks were rated using a risk evaluation process that accounted for changes in risk from the prior year, and were formally documented, along with mitigation strategies, for management review during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.1.2	Assigned risk owners select and develop control activities to mitigate the risks identified during the annual risk assessment process. The control activities are documented within risk treatment plans that are created by the risk owners for risks above the tolerable threshold.	Inspected the most recently completed risk assessment documentation to determine that assigned risk owners selected and developed control activities to mitigate the risks identified as part of the risk assessment process and that the control activities were documented within risk treatment plans that were created by the risk owners for risks above the tolerable threshold during the period.	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	Assigned risk owners select and develop control activities to mitigate the risks identified during the annual risk assessment process. The control activities are documented within risk treatment plans that are created by the risk owners for risks above the tolerable threshold.	Inspected the most recently completed risk assessment documentation to determine that assigned risk owners selected and developed control activities to mitigate the risks identified as part of the risk assessment process and that the control activities were documented within risk treatment plans that were created by the risk owners for risks above the tolerable threshold during the period.	No exceptions noted.
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	Information system security and data classification and handling policies are formally documented that identify information required to support the functioning of internal control and achievement of objectives and associated protection and access rights.	Inspected the information security and data classification policies and procedures to determine that information system security and data classification and handling policies were formally documented that identified information required to support the functioning of internal control and achievement of objectives and associated protection and access rights.	No exceptions noted.
CC5.3.2	Operating policies and procedures are documented, updated on an annual basis, and communicated to relevant stakeholders that define information system baseline requirements, establish and monitor alarm levels, and select measures, analytic techniques, and tools to be used in managing system security.	Inspected the information security policy available to stakeholders via the company website to determine that operating policies and procedures were documented, updated, and communicated to relevant stakeholders that defined information system baseline requirements, established and monitored alarm levels, and selected measures, analytic techniques, and tools to be used in managing system security during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.3.3	An employee sanction policy is in place communicating that an employee may be terminated for noncompliance with a policy and/or procedure.	Inspected the employee sanction policies and procedures to determine that an employee sanction policy was in place communicating that an employee may be terminated for noncompliance with a policy and/or procedure.	No exceptions noted.
CC5.3.4	Information system security and data classification and handling policies are formally documented that identify information required to support the functioning of internal control and achievement of objectives and associated protection and access rights.	Inspected the information security and data classification policies and procedures to determine that information system security and data classification and handling policies were formally documented that identified information required to support the functioning of internal control and achievement of objectives and associated protection and access rights.	No exceptions noted.
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	The engineering team has formally documented standard build procedures for installation and maintenance of production servers that includes the requirement for access control systems to enforce logical access.	Inspected the standard build procedures to determine that the engineering team had formally documented standard build procedures for installation and maintenance of production servers that included the requirement for access control systems to enforce logical access.	No exceptions noted.
CC6.1.2	The in-scope systems are configured to authenticate users with a user account and enforce predefined user account and minimum password requirements or SSH public key authentication, and to enforce MFA as applicable.	<p>Inspected the user account listing and the authentication configurations for a sample of in-scope systems to determine that the following sampled in-scope systems were configured to authenticate users with a user account and enforce predefined user account and minimum password requirements or SSH public key authentication, and to enforce MFA as applicable:</p> <ul style="list-style-type: none"> • Identity management service • Infrastructure management console • Bastion host • Production containers • Production servers • Production databases • VPN 	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.3	Predefined security groups are utilized to assign role-based access privileges and restrict access to data to the in-scope systems.	<p>Inspected the administrative user account listings for a sample of in-scope systems to determine that predefined security groups were utilized to assign role-based access privileges and restrict access to data for the following sampled in-scope systems:</p> <ul style="list-style-type: none"> • Identity management service • Infrastructure management console • Bastion host • Production containers • Production servers • Production databases • VPN 	No exceptions noted.
CC6.1.4	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel.	<p>Inspected the administrator user account listings for a sample of in-scope systems with the assistance of the CTO to determine that administrative access privileges to the following sampled in-scope systems were restricted to user accounts accessible by authorized personnel:</p> <ul style="list-style-type: none"> • Identity management service • Infrastructure management console • Bastion host • Production containers • Production servers • Production databases • VPN 	No exceptions noted.
CC6.1.5	The production network is segmented to help ensure that confidential data is isolated from other unrelated networks.	Inspected the network configurations to determine that the production network was segmented to ensure that confidential data was isolated from other unrelated networks.	No exceptions noted.
CC6.1.6	Confidential data is stored in an encrypted format utilizing AES-256. Access to manage cryptographic keys is restricted to user accounts accessible by authorized personnel.	Inspected the encryption configurations for a sample of production databases and the listing of user accounts with access to manage the cryptographic keys with the assistance of the CTO to determine that confidential data was stored in an encrypted format utilizing AES-256 and that access to manage cryptographic keys was restricted to user accounts accessible by authorized personnel for each database sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	AWS is responsible for implementing controls to manage logical access to the underlying network, virtualization management software, and storage devices for its cloud hosting services where the OneNotary 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	Internal user access requests are documented in an access request task and require manager approval prior to access being granted.	Inquired of the compliance consultant regarding user access requests to determine that internal user access requests were documented in an access request task and approved by a manager prior to access being granted.	No exceptions noted.
		Inspected the access request ticketing documentation for a sample of user access requests during the period to determine that each user access request sampled was documented in an access request task and was approved by a manager.	No exceptions noted.
CC6.2.2	Termination checklists are completed and system access is revoked for employees as a component of the employee termination process.	Inspected the termination checklist and the user account listing for a sample of in-scope systems and employees terminated during the period to determine that termination checklists were completed and system access was revoked as a component of the employee termination process for each in-scope system and terminated employee sampled: <ul style="list-style-type: none"> • Identity management service • Infrastructure management console • Bastion host • Production containers • Production servers • Production databases • VPN 	No exceptions noted.
CC6.2.3	User access reviews, including privileged users, are performed by management on a quarterly basis to help ensure that access to data is restricted and authorized. Accounts identified as inappropriate are investigated and resolved.	Inquired of the compliance consultant regarding user access reviews to determine that user access reviews, including privileged users, were performed by management on a quarterly basis to ensure that access to data was restricted and authorized and that accounts identified as inappropriate were investigated and resolved.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the user access review documentation for a sample of quarters during the period to determine that user access reviews, including privileged users, were performed by management for each quarter sampled to ensure that access to data was restricted and authorized and that accounts identified as inappropriate were investigated and resolved.	No exceptions noted.
AWS is responsible for implementing controls to manage logical access to the underlying network, virtualization management software, and storage devices for its cloud hosting services where the OneNotary 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	Internal user access requests are documented in an access request task and require manager approval prior to access being granted.	Inquired of the compliance consultant regarding user access requests to determine that internal user access requests were documented in an access request task and approved by a manager prior to access being granted.	No exceptions noted.
		Inspected the access request ticketing documentation for a sample of user access requests during the period to determine that each user access request sampled was documented in an access request task and was approved by a manager.	No exceptions noted.
CC6.3.2	Termination checklists are completed and system access is revoked for employees as a component of the employee termination process.	<p>Inspected the termination checklist and the user account listing for a sample of in-scope systems and employees terminated during the period to determine that termination checklists were completed and system access was revoked as a component of the employee termination process for each in-scope system and terminated employee sampled:</p> <ul style="list-style-type: none"> • Identity management service • Infrastructure management console • Bastion host • Production containers • Production servers • Production databases • VPN 	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.3.3	Predefined security groups are utilized to assign role-based access privileges and restrict access to data to the in-scope systems.	<p>Inspected the administrative user account listings for a sample of in-scope systems to determine that predefined security groups were utilized to assign role-based access privileges and restrict access to data for the following sampled in-scope systems:</p> <ul style="list-style-type: none"> • Identity management service • Infrastructure management console • Bastion host • Production containers • Production servers • Production databases • VPN 	No exceptions noted.
CC6.3.4	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel.	<p>Inspected the administrator user account listings for a sample of in-scope systems with the assistance of the CTO to determine that administrative access privileges to the following sampled in-scope systems were restricted to user accounts accessible by authorized personnel:</p> <ul style="list-style-type: none"> • Identity management service • Infrastructure management console • Bastion host • Production containers • Production servers • Production databases • VPN 	No exceptions noted.
CC6.3.5	User access reviews, including privileged users, are performed by management on a quarterly basis to help ensure that access to data is restricted and authorized. Accounts identified as inappropriate are investigated and resolved.	Inquired of the compliance consultant regarding user access reviews to determine that user access reviews, including privileged users, were performed by management on a quarterly basis to ensure that access to data was restricted and authorized and that accounts identified as inappropriate were investigated and resolved.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the user access review documentation for a sample of quarters during the period to determine that user access reviews, including privileged users, were performed by management for each quarter sampled to ensure that access to data was restricted and authorized and that accounts identified as inappropriate were investigated and resolved.	No exceptions noted.
	AWS is responsible for implementing controls to manage logical access to the underlying network, virtualization management software, and storage devices for its cloud hosting services where the OneNotary systems reside.		
CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
	AWS is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.		
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.			
	AWS is responsible for implementing controls to manage logical access to the underlying network, virtualization management software, and storage devices for its cloud hosting services where the OneNotary systems reside.		
	AWS is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.		
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	Security groups are configured to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized by a rule.	Inspected the security group configurations to determine that security groups were configured to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that was not explicitly authorized by a rule.	No exceptions noted.
CC6.6.2	Security groups are reviewed on a quarterly basis to help ensure that only necessary connections are configured.	Inspected the security group review documentation for a sample of quarters during the period to determine that security groups were reviewed for each quarter sampled to ensure that only necessary connections were configured.	No exceptions noted.
CC6.6.3	Web servers utilize TLS 1.2 encryption protocol for web communication sessions.	Inspected the TLS certificate configurations to determine that web servers utilized TLS 1.2 encryption protocol for web communication sessions.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.6.4	An encrypted VPN is required for remote access to the production network domain. Production network domain users are required to authenticate via an OneNotary-issued certificate before being granted access to the production network domain.	Inspected the VPN encryption configurations and production network domain authentication configurations to determine that an encrypted VPN was required for remote access to the production network domain and users were required to authenticate via an OneNotary-issued certificate before being granted access to the production network domain.	No exceptions noted.
CC6.6.5	An IDS is configured to report network events related to suspected or actual unauthorized access from outside the system boundaries. Notifications are sent to engineering personnel via the internal collaboration tool to analyze and respond to events.	Inspected the IDS configurations and an example alert generated during the period to determine that an IDS was configured to report network events related to suspected or actual unauthorized access from outside the system boundaries and that notifications were sent to engineering personnel via the internal collaboration tool to analyze and respond to events.	No exceptions noted.
CC6.6.6	An automated monitoring tool is configured to monitor AWS security group changes and send alerts to engineering personnel via the internal collaboration tool upon detected configuration changes.	Inspected the monitoring tool configurations and an example alert generated during the period to determine that an automated monitoring tool was configured to monitor AWS security group changes and send alerts to engineering personnel via the internal collaboration tool upon detected configuration changes.	No exceptions noted.
CC6.6.7	Penetration testing is performed by a third-party vendor on an annual basis. Security vulnerabilities that are identified are triaged by the security team and monitored through resolution.	Inspected the most recent penetration testing report and an example vulnerability remediation ticket resolved during the period to determine that penetration testing was performed by a third-party vendor and that security vulnerabilities that were identified were triaged by the security team and monitored through resolution during the period.	No exceptions noted.
CC6.6.8	Vulnerability assessments are performed on at least a monthly basis. Security vulnerabilities that are identified are triaged by the security team and monitored through resolution.	Inquired of the compliance consultant regarding vulnerability assessments to determine that vulnerability assessments were performed on at least a monthly basis and that security vulnerabilities that were identified were triaged by the security team and monitored through resolution.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the vulnerability assessment documentation for a sample of months during the period and an example vulnerability remediation ticket resolved during the period to determine that vulnerability assessments were performed and that security vulnerabilities that were identified were triaged by the security team and monitored through resolution for each month sampled.	No exceptions noted.
AWS is responsible for implementing controls to manage logical access to the underlying network, virtualization management software, and storage devices for its cloud hosting services where the OneNotary 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	Documented policies and procedures are in place that prohibit the transmission of sensitive information over the Internet or other public communications paths unless it is encrypted.	Inspected the encryption policy to determine that documented policies and procedures were in place that prohibited the transmission of sensitive information over the Internet or other public communications paths unless it was encrypted.	No exceptions noted.
CC6.7.2	An encrypted VPN is required for remote access to the production network domain. Production network domain users are required to authenticate via an OneNotary-issued certificate before being granted access to the production network domain.	Inspected the VPN encryption configurations and production network domain authentication configurations to determine that an encrypted VPN was required for remote access to the production network domain and users were required to authenticate via an OneNotary-issued certificate before being granted access to the production network domain.	No exceptions noted.
CC6.7.3	Web servers utilize TLS 1.2 encryption protocol for web communication sessions.	Inspected the TLS certificate configurations to determine that web servers utilized TLS 1.2 encryption protocol for web communication sessions.	No exceptions noted.
CC6.7.4	Confidential data is stored in an encrypted format utilizing AES-256. Access to manage cryptographic keys is restricted to user accounts accessible by authorized personnel.	Inspected the encryption configurations for a sample of production databases and the listing of user accounts with access to manage the cryptographic keys with the assistance of the CTO to determine that confidential data was stored in an encrypted format utilizing AES-256 and that access to manage cryptographic keys was restricted to user accounts accessible by authorized personnel for each database sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.7.5	MDM software is configured to encrypt the hard drives of OneNotary-owned workstations.	Inspected the MDM software encryption configurations, the listing of managed workstations, and an example employee workstation to determine that MDM software was configured to encrypt the hard drives of OneNotary-owned workstations.	No exceptions noted.
AWS is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where the OneNotary systems reside.			
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	Linux-based technology and software architecture is in place which minimizes the risk of production servers being infected by computer viruses, malicious code, and unauthorized software.	Inspected the Linux-based technology and software architecture for a sample of production servers to determine that Linux-based technology and software architecture was in place which minimized the risk of production servers being infected by computer viruses, malicious code, and unauthorized software for each server sampled.	No exceptions noted.
CC6.8.2	The ability to install applications or software is restricted to authorized engineering personnel.	Inspected the listing of user accounts with the ability to install applications or software for a sample of in-scope systems with the assistance of the CTO to determine that the ability to install applications or software was restricted to authorized engineering personnel for each in-scope system sampled.	No exceptions noted.
CC6.8.3	MDM software is configured to install and manage enterprise anti-malware software on OneNotary-owned workstations.	Inspected the MDM software configurations, the anti-malware software configurations, the listing of managed workstations, and an example employee workstation to determine that MDM software was configured to install and manage enterprise anti-malware software on OneNotary-owned workstations.	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 engineering team has formally documented standard build procedures for installation and maintenance of production servers that includes the requirement for access control systems to enforce logical access.	Inspected the standard build procedures to determine that the engineering team had formally documented standard build procedures for installation and maintenance of production servers that included the requirement for access control systems to enforce logical access.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.1.2	Penetration testing is performed by a third-party vendor on an annual basis. Security vulnerabilities that are identified are triaged by the security team and monitored through resolution.	Inspected the most recent penetration testing report and an example vulnerability remediation ticket resolved during the period to determine that penetration testing was performed by a third-party vendor and that security vulnerabilities that were identified were triaged by the security team and monitored through resolution during the period.	No exceptions noted.
CC7.1.3	Vulnerability assessments are performed on at least a monthly basis. Security vulnerabilities that are identified are triaged by the security team and monitored through resolution.	Inquired of the compliance consultant regarding vulnerability assessments to determine that vulnerability assessments were performed on at least a monthly basis and that security vulnerabilities that were identified were triaged by the security team and monitored through resolution.	No exceptions noted.
		Inspected the vulnerability assessment documentation for a sample of months during the period and an example vulnerability remediation ticket resolved during the period to determine that vulnerability assessments were performed and that security vulnerabilities that were identified were triaged by the security team and monitored through resolution for each month sampled.	No exceptions noted.
CC7.1.4	Logging and monitoring software is configured to collect data from system infrastructure components and endpoint systems to monitor system performance, potential security vulnerabilities, and resource utilization, and to alert the engineering team upon detection of unusual system activity or service requests.	Inspected the logging and monitoring software configurations and example alerts generated during the period to determine that logging and monitoring software was configured to collect data from system infrastructure components and endpoint systems to monitor system performance, potential security vulnerabilities, and resource utilization, and to alert the engineering team upon detection of unusual system activity or service requests.	No exceptions noted.
CC7.1.5	An automated monitoring tool is configured to monitor AWS security group changes and send alerts to engineering personnel via the internal collaboration tool upon detected configuration changes.	Inspected the monitoring tool configurations and an example alert generated during the period to determine that an automated monitoring tool was configured to monitor AWS security group changes and send alerts to engineering personnel via the internal collaboration tool upon detected configuration changes.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.1.6	Security groups are reviewed on a quarterly basis to help ensure that only necessary connections are configured.	Inspected the security group review documentation for a sample of quarters during the period to determine that security groups were reviewed for each quarter sampled to ensure that only necessary connections were configured.	No exceptions noted.
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC7.2.1	Logging and monitoring software is configured to collect data from system infrastructure components and endpoint systems to monitor system performance, potential security vulnerabilities, and resource utilization, and to alert the engineering team upon detection of unusual system activity or service requests.	Inspected the logging and monitoring software configurations and example alerts generated during the period to determine that logging and monitoring software was configured to collect data from system infrastructure components and endpoint systems to monitor system performance, potential security vulnerabilities, and resource utilization, and to alert the engineering team upon detection of unusual system activity or service requests.	No exceptions noted.
CC7.2.2	An IDS is configured to report network events related to suspected or actual unauthorized access from outside the system boundaries. Notifications are sent to engineering personnel via the internal collaboration tool to analyze and respond to events.	Inspected the IDS configurations and an example alert generated during the period to determine that an IDS was configured to report network events related to suspected or actual unauthorized access from outside the system boundaries and that notifications were sent to engineering personnel via the internal collaboration tool to analyze and respond to events.	No exceptions noted.
CC7.2.3	Penetration testing is performed by a third-party vendor on an annual basis. Security vulnerabilities that are identified are triaged by the security team and monitored through resolution.	Inspected the most recent penetration testing report and an example vulnerability remediation ticket resolved during the period to determine that penetration testing was performed by a third-party vendor and that security vulnerabilities that were identified were triaged by the security team and monitored through resolution during the period.	No exceptions noted.
CC7.2.4	Vulnerability assessments are performed on at least a monthly basis. Security vulnerabilities that are identified are triaged by the security team and monitored through resolution.	Inquired of the compliance consultant regarding vulnerability assessments to determine that vulnerability assessments were performed on at least a monthly basis and that security vulnerabilities that were identified were triaged by the security team and monitored through resolution.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the vulnerability assessment documentation for a sample of months during the period and an example vulnerability remediation ticket resolved during the period to determine that vulnerability assessments were performed and that security vulnerabilities that were identified were triaged by the security team and monitored through resolution for each month sampled.	No exceptions noted.
AWS is responsible for monitoring the logical access control systems for the underlying network, virtualization management software, and storage devices for its cloud hosting services where the OneNotary systems reside.			
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	Incident response procedures are in place that outline the response procedures to security events and include lessons learned to evaluate the effectiveness of the procedures. The procedures are reviewed on an annual basis to help ensure they are effectively meeting the business objectives.	Inspected the incident response policies and procedures to determine that incident response procedures were in place that outlined the response procedures to security events and included lessons learned to evaluate the effectiveness of the procedures and that the procedures were reviewed to ensure they were effectively meeting the business objectives during the period.	No exceptions noted.
CC7.3.2	Reported or detected security incidents are tracked within a tracking system until resolved. Closed security incidents are reviewed and approved by management to help ensure that the incident response procedures were followed, and that the incident was resolved.	Inspected the listing of security incidents during the period with the assistance of the compliance consultant and determined that no security incidents occurred during the period; therefore, no testing of operating effectiveness was performed.	
CC7.3.3	Security management meetings are held on a quarterly basis to discuss the effect of identified security vulnerabilities on the ability to meet business objectives and to identify corrective measures.	Inquired of the compliance consultant regarding security management meetings to determine that security management meetings were held on a quarterly basis to discuss the effect of identified security vulnerabilities on the ability to meet business objectives and to identify corrective measures.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the security management meeting calendar invite and presentation slide deck for a sample of quarters during the period to determine that security management meetings were held to discuss the effect of identified security vulnerabilities on the ability to meet business objectives and to identify corrective measures for each quarter sampled.	No exceptions noted.
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	Incident response procedures are in place that outline the response procedures to security events and include lessons learned to evaluate the effectiveness of the procedures. The procedures are reviewed on an annual basis to help ensure they are effectively meeting the business objectives.	Inspected the incident response policies and procedures to determine that incident response procedures were in place that outlined the response procedures to security events and included lessons learned to evaluate the effectiveness of the procedures and that the procedures were reviewed to ensure they were effectively meeting the business objectives during the period.	No exceptions noted.
CC7.4.2	Reported or detected security incidents are tracked within a tracking system until resolved. Closed security incidents are reviewed and approved by management to help ensure that the incident response procedures were followed, and that the incident was resolved.	Inspected the listing of security incidents during the period with the assistance of the compliance consultant and determined that no security incidents occurred during the period; therefore, no testing of operating effectiveness was performed.	
CC7.4.3	Security management meetings are held on a quarterly basis to discuss the effect of identified security vulnerabilities on the ability to meet business objectives and to identify corrective measures.	Inquired of the compliance consultant regarding security management meetings to determine that security management meetings were held on a quarterly basis to discuss the effect of identified security vulnerabilities on the ability to meet business objectives and to identify corrective measures.	No exceptions noted.
		Inspected the security management meeting calendar invite and presentation slide deck for a sample of quarters during the period to determine that security management meetings were held to discuss the effect of identified security vulnerabilities on the ability to meet business objectives and to identify corrective measures for each quarter sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	<p>Documented incident response procedures are in place that include the following to guide personnel throughout the incident response process:</p> <ul style="list-style-type: none"> • Remediation of the incident • Restoration of operations • Communication protocols and timing to affected parties • Lessons learned 	<p>Inspected the incident response plan to determine that documented incident response procedures were in place that included the following to guide personnel throughout the incident response process:</p> <ul style="list-style-type: none"> • Remediation of the incident • Restoration of operations • Communication protocols and timing to affected parties • Lessons learned 	No exceptions noted.
CC7.5.2	<p>Reported or detected security incidents are tracked within a tracking system until resolved. Closed security incidents are reviewed and approved by management to help ensure that the incident response procedures were followed, and that the incident was resolved.</p>	<p>Inspected the listing of security incidents during the period with the assistance of the compliance consultant and determined that no security incidents occurred during the period; therefore, no testing of operating effectiveness was performed.</p>	
CC7.5.3	<p>Engineering personnel complete incident postmortem reports upon system outages that include the incident and impact analysis, resolutions, lessons learned, and action items.</p>	<p>Inspected the listing of security incidents during the period with the assistance of the compliance consultant and determined that no security incidents occurred during the period; therefore, no testing of operating effectiveness was performed.</p>	
CC7.5.4	<p>Security management meetings are held on a quarterly basis to discuss the effect of identified security vulnerabilities on the ability to meet business objectives and to identify corrective measures.</p>	<p>Inquired of the compliance consultant regarding security management meetings to determine that security management meetings were held on a quarterly basis to discuss the effect of identified security vulnerabilities on the ability to meet business objectives and to identify corrective measures.</p>	No exceptions noted.
		<p>Inspected the security management meeting calendar invite and presentation slide deck for a sample of quarters during the period to determine that security management meetings were held to discuss the effect of identified security vulnerabilities on the ability to meet business objectives and to identify corrective measures for each quarter sampled.</p>	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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	Change management policies and procedures are in place to guide personnel in the request, documentation, testing, and approval of changes.	Inspected the change management policies and procedures to determine that change management policies and procedures were in place to guide personnel in the request, documentation, testing, and approval of changes.	No exceptions noted.
CC8.1.2	Engineering team meetings are held on a quarterly basis to discuss and communicate the ongoing and upcoming projects that affect the system.	Inspected the engineering team meeting calendar invitation and the meeting minutes for a sample of quarters during the period to determine that engineering team meetings were held for each quarter sampled to discuss and communicate the ongoing and upcoming projects that affect the system.	No exceptions noted.
CC8.1.3	Changes made to in-scope systems are authorized, peer reviewed, tested, and approved prior to implementation.	Inquired of the CTO regarding the change management process to determine that changes made to in-scope systems were authorized, peer reviewed, tested, and approved prior to implementation.	No exceptions noted.
		Inspected the change documentation for a sample of application and infrastructure changes implemented during the period to determine that each change sampled was authorized, peer reviewed, tested, and approved.	No exceptions noted.
CC8.1.4	The production environment is logically segmented from development and test environments.	Inspected the network configurations to determine that the production environment was logically segmented from development and test environments.	No exceptions noted.
CC8.1.5	Version control software is utilized to restrict access to application source code and provide rollback capabilities.	Inspected the version control software configurations and user account listing to determine that version control software was utilized to restrict access to application source code and provide rollback capabilities.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.1.6	Write access privileges to the version control software are restricted to user accounts accessible by authorized personnel.	Inspected the administrator user account listing and the listing of user accounts with write access privileges for a sample of in-scope repositories with the assistance of the CTO to determine that write access privileges to the version control software were restricted to user accounts accessible by authorized personnel for each repository sampled.	No exceptions noted.
CC8.1.7	The version control software is configured to restrict users from merging code without peer approval, thus preventing any one user from both developing and implementing code to the production environment.	Inquired of the CTO regarding branch protection configurations to determine that the version control software was configured to restrict users from merging code without peer approval, thus preventing any one user from both developing and implementing code to the production environment.	The test of the control activity disclosed that the peer approval requirement configured within the version control software branch protection configurations was implemented on November 30, 2023.
		Inspected the version control software branch protection configurations for a sample of in-scope repositories to determine that the version control software was configured to restrict users from merging code without peer approval, thus preventing any one user from both developing and implementing code to the production environment for each repository sampled.	No exceptions noted.
CC8.1.8	Administrative access privileges within the version control software are restricted to user accounts accessible by authorized personnel.	Inspected the version control software administrator user account listing with the assistance of the CTO to determine that administrative access privileges within the version control software were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC8.1.9	The ability to implement changes into the production environment is restricted to user accounts accessible by authorized personnel.	Inspected the listing of user accounts with the ability to implement changes to the production environment for a sample of in-scope repositories with the assistance of the CTO to determine that the ability to implement changes into the production environment was restricted to user accounts accessible by authorized personnel for each repository sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.1.10	OneNotary management monitors for application changes deployed outside of the standard change management process on a daily basis. Exceptions are investigated and logged.	Inquired of the CTO regarding change management review to determine that OneNotary management monitored for application changes deployed outside of the standard change management process on a daily basis and that exceptions that were identified were investigated and logged.	No exceptions noted.
		Inspected the evidence of application change review for a sample of days during the period to determine that OneNotary management monitored for application changes deployed outside of the standard change management process on a daily basis and that exceptions that were identified were investigated and logged for each day sampled.	No exceptions noted.
CC8.1.11	Customer data is not utilized for application change control development or testing.	Inquired of the CTO to determine that customer data was not utilized for application change control development or testing.	No exceptions noted.
		Inspected example testing data utilized during the period to determine that customer data was not utilized for application change control development or testing.	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	Documented policies and procedures are in place to guide personnel in identifying, selecting, and developing risk management strategies specifically addressing the risks arising from potential business disruptions as part of the risk assessment process.	Inspected the risk management policy to determine that documented policies and procedures were in place to guide personnel in identifying, selecting, and developing risk management strategies specifically addressing the risks arising from potential business disruptions as part of the risk assessment process.	No exceptions noted.
CC9.1.2	Disaster recovery and business continuity plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event and are reviewed and approved on an annual basis.	Inspected the disaster recovery policy and procedures to determine that disaster recovery and business continuity plans were in place to guide personnel against disruptions caused by an unexpected event and was reviewed and approved during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.1.3	Business continuity and disaster recovery plans are tested on an annual basis to help ensure the production environment can be recovered in the event of a disaster.	Inspected the most recently completed business continuity and disaster recovery test results to determine that business continuity and disaster recovery plans were tested to ensure the production environment could be recovered in the event of a disaster during the period.	No exceptions noted.
CC9.1.4	A formal risk assessment is performed on an annual basis that considers risks arising from internal and external factors, including business disruptions, vendors, and the potential for fraud. Risks that are identified are rated using a risk evaluation process that accounts for changes in risk from the prior year, and are formally documented, along with mitigation strategies, for management review.	Inquired of the compliance consultant regarding risks from vendors to determine that a formal risk assessment was performed during the period that considered risks arising from vendors.	No exceptions noted.
		Inspected the most recently completed risk assessment documentation to determine that a formal risk assessment was performed that considered the risks that arise from internal and external factors, including risks arising from potential business disruptions, and the potential for fraud, and that identified risks were rated using a risk evaluation process that accounted for changes in risk from the prior year, and were formally documented, along with mitigation strategies, for management review during the period.	No exceptions noted.
CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	Documented vendor management policies and procedures are in place to guide personnel in assessing and managing risks associated with third parties.	Inspected the vendor management policies and procedures to determine that documented vendor management policies and procedures were in place to guide personnel in assessing and managing risks associated with third parties.	No exceptions noted
CC9.2.2	Nondisclosure agreements of confidentiality and protection are required before sharing information designated as confidential with third parties.	Inspected the nondisclosure agreements for a sample of third-party vendors and the standard customer agreement to determine that nondisclosure agreements of confidentiality and protection were in place before sharing information designated as confidential with third parties for each third party sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.2.3	A formal risk assessment is performed on an annual basis that considers risks arising from internal and external factors, including business disruptions, vendors, and the potential for fraud. Risks that are identified are rated using a risk evaluation process that accounts for changes in risk from the prior year, and are formally documented, along with mitigation strategies, for management review.	Inquired of the compliance consultant regarding risks from vendors to determine that a formal risk assessment was performed during the period that considered risks arising from vendors.	No exceptions noted.
		Inspected the most recently completed risk assessment documentation to determine that a formal risk assessment was performed that considered the risks that arise from internal and external factors, including risks arising from potential business disruptions, and the potential for fraud, and that identified risks were rated using a risk evaluation process that accounted for changes in risk from the prior year, and were formally documented, along with mitigation strategies, for management review during the period.	No exceptions noted.
CC9.2.4	Management obtains and reviews vendor audit reports on an annual basis to help ensure that third-party service providers are in compliance with the organization's requirements.	Inspected the vendor assessment for a sample of vendors to determine that management obtained and reviewed vendor audit reports during the period to ensure that third-party service providers were in compliance with the organization's requirements for each third-party sampled.	No exceptions noted.