Insight Assurance

Delivering Quality, Assuring Trust.

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

Report on OneMeta Inc.'s Description of Its Verbum Suite and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security Throughout the Period August 1, 2024, to October 31, 2024

OneMeta™

TABLE OF CONTENTS

SECTION 1: INDEPENDENT SERVICE AUDITOR'S REPORT

Insight Assurance
Delivering Quality, Assuring Trust.

INDEPENDENT SERVICE AUDITOR'S REPORT

To: OneMeta Inc.

Scope

We have examined OneMeta Inc.'s ("OneMeta" or "the Service Organization") description of its Verbum Suite found in Section 3 titled "OneMeta Inc.'s description of its Verbum Suite" throughout the period August 1, 2024, to October 31, 2024, ("description") based on the criteria for a description of a service organization's system set forth in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)* in AICPA, *Description Criteria*, (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period August 1, 2024, to October 31, 2024, to provide reasonable assurance that OneMeta's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA*, Trust Services Criteria.*

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

The information included in Section 5 "Other Information Provided by OneMeta Inc." is presented by management of OneMeta to provide additional information and is not part of OneMeta Inc.'s description. Information about OneMeta management responses to exceptions has not been subjected to the procedures applied in the examination of the description and the suitability of the design and operating effectiveness of controls to meet the applicable trust services criteria, and accordingly, we do not express an opinion on it.

Service Organization's Responsibilities

OneMeta is responsible for its service commitments and system requirements and designing, implementing, and operating effective controls within the system to provide reasonable assurance that OneMeta's service commitments and system requirements were achieved. In Section 2, OneMeta has provided the accompanying assertion titled "OneMeta Inc.'s Management Assertion" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. OneMeta 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 the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

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

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls.

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

Emphasis of Matter – Controls Did Not Operate During the Period Covered by the Report

The Service Organization's description of its system discusses its security incident response and recovery procedures. However, during the period August 1, 2024, to October 31, 2024, the Service Organization did not experience a security incident that would warrant the operation of this control. Because this control did not operate during the period, we were unable to test, and did not test, the operating effectiveness of those controls as evaluated using the following trust services criteria:

- 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.*
- CC7.5, *The entity identifies, develops, and implements activities to recover from identified security incidents.*

Our opinion is not modified with respect to the matter emphasized.

Description of Test of Controls

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

Opinion

In our opinion, in all material respects,

- the description presents OneMeta's Verbum Suite that was designed and implemented throughout the period August 1, 2024, to October 31, 2024, in accordance with the description criteria.
- the controls stated in the description were suitably designed throughout the period August 1, 2024, to October 31, 2024, to provide reasonable assurance that OneMeta'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 OneMeta's controls throughout that period.
- the controls stated in the description operated effectively throughout the period August 1, 2024, to October 31, 2024, to provide reasonable assurance that OneMeta'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 OneMeta's controls operated effectively throughout that period.

Restricted Use

This report is intended solely for the information and use of OneMeta, user entities of OneMeta's Verbum Suite throughout the period August 1, 2024, to October 31, 2024, and business partners of OneMeta subject to risks arising from interactions with the Verbum Suite, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

Insight Assurance LLC

Tampa, Florida
May 8, 2025

SECTION 2: ONEMETA INC.'S MANAGEMENT ASSERTION

OneMeta™

ONEMETA INC.'S MANAGEMENT ASSERTION

We have prepared the description of OneMeta Inc.'s ("OneMeta" or "the Service Organization") Verbum Suite entitled "OneMeta Inc.'s description of its Verbum Suite" throughout the period August 1, 2024, to October 31, 2024, ("description") based on the criteria for a description of a service organization's system set forth in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)* in AICPA, *Description Criteria*, (description criteria) The description is intended to provide report users with information about the Verbum Suite that may be useful when assessing the risks arising from interactions with OneMeta's system, particularly information about system controls that OneMeta has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA*, Trust Services Criteria.*

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

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

- the description presents OneMeta's Verbum Suite that was designed and implemented throughout the period August 1, 2024, to October 31, 2024, in accordance with the description criteria.
- the controls stated in the description were suitably designed throughout the period August 1, 2024, to October 31, 2024, to provide reasonable assurance that OneMeta's service commitments and system requirements would be achieved based on the applicable trust services criteria, and if the subservice organization and user entities applied the complementary controls assumed in the design of OneMeta's controls.
- the controls stated in the description operated effectively throughout the period August 1, 2024, to October 31, 2024, to provide reasonable assurance that OneMeta'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 OneMeta's controls operated effectively throughout that period.

OneMeta Inc.
May 8, 2025

SECTION 3: ONEMETA INC.'S DESCRIPTION OF ITS VERBUM SUITE

ONEMETA INC.'S DESCRIPTION OF ITS VERBUM SUITE

COMPANY BACKGROUND

OneMeta, Inc. ("OneMeta") is a publicly held company established in 2009 that offers software Services. OneMeta is a Nevada Corporation headquartered in Bountiful, Utah.

DESCRIPTION OF SERVICES OVERVIEW

OneMeta provides a suite of communication products—**VerbumCall, VerbumMeeting, VerbumOnsite, Verbum Transcript, and Verbum API**—that enable real-time multilingual translation, transcription, and interpretation. These services leverage AI and natural language processing (NLP) technologies to facilitate cross-language communication.

Key System Components:

- **VerbumCall:** Real-time translation and transcription for phone calls, supporting multiple languages and integration with call center systems.
- **VerbumMeeting:** Real-time interpretation and transcription for video conferences, compatible with multiple platforms and scalable for enterprise use.
- **VerbumOnsite:** Onsite interpretation services for events, utilizing proprietary hardware and software.
- **Verbum Transcript:** A web-based platform for transcribing and translating audio/video files, supporting over 125 languages.
- **Verbum API:** Allows integration of real-time translation into third-party applications.**:**

The system implements industry-standard controls for data security, including encryption, access management, and audit logging, to protect multilingual communications during processing.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

OneMeta designs its processes and procedures related to OneMeta's Verbum Suite ("System") to meet its objectives. Those objectives are based on the service commitments that OneMeta makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that OneMeta has established for the services.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offered online.

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

- Security principles within the fundamental designs of services are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Use of encryption technologies to protect customer data both at rest and in transit.
- Use of data retention and data disposal
- Uptime availability of production systems

OneMeta establishes operational requirements that support the achievement of security, relevant laws and regulations, and other system requirements. Such requirements are communicated in system policies and procedures, system design documentation, and agreements with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition, how to carry out specific manual and automated processes required in the operation and development of the System.

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

The System description is comprised of the following components:

- *Infrastructure* – The collection of physical or virtual resources that supports an overall IT environment, including the physical environment and related structures, IT and hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile devices, and internal networks and connected external telecommunications networks) that the Company used to provide the services.
- *Software* - The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile or desktop/laptop applications.
- *People* - The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- *Data* – The types of data used by the system, such as transaction streams, files, databases, tables, and output used or processed by the system.
- *Procedures* – The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

INFRASTRUCTURE

OneMeta's infrastructure is a robust and scalable cloud-based ecosystem that leverages state-of-the-art technologies. It employs Microsoft Azure (‘Azure’) for cloud services, which provide the backbone for its AI and NLP capabilities. In addition to this, OneMeta utilizes Vonage Communication for VOIP and video streaming services, further enhancing its product offerings across multiple industries. This advanced infrastructure allows OneMeta to deliver secure, efficient, and high-quality solutions to its OneMeta.

The OneMeta application infrastructure is located in Azure cloud services. Azure acts as a hosting subservice organization for the company. The subservice organization provides physical security and environmental protection controls, as well as managed services for OneMeta’s infrastructure.

Azure’s network security uses hardware and software-based intrusion prevention, advanced content filtering, anti-malware, and anti-spam modules.

In addition to the firewall, OneMeta uses anti-virus and anti-spyware applications to protect systems from viruses.

OneMeta's Information Security Policy and security procedures ensure that all computer devices (including servers, desktops, printers, etc.) connected to the OneMeta network have proper virus protection software, current virus definition libraries, and the most recent operating system and security patches installed. The IT department verifies that all known and reasonable defenses are in place to reduce network vulnerabilities while keeping the network operating. In the event of a virus threat, the anti-virus system will attempt to delete or quarantine the infected file. If the virus cannot be deleted or quarantined, the infected machine will be disconnected from the network and cleaned manually.

Multiple controls are installed to monitor traffic that could contain malicious programs or code. External perimeter scans are performed annually by a third-party vendor to expose potential vulnerabilities to the production environment and corporate data. Email is scanned at the gateway and in the hosted email environment. Server operating systems utilize anti-virus and anti-spyware programs. All employee workstation computers have a minimum standard hardware and software configuration. Employees are not allowed to install any software on OneMeta-owned computers. IT staff maintain several replacement computers that can replace workstations in need of repair or maintenance, thereby disrupting the employees' workday as little as possible.

SOFTWARE

OneMeta maintains a list of critical software in use within its environment. The organization also retains appropriate software license documentation.

Primary Software		
System/Application	**Operating System**	**Purpose**
Verbum Suite	Linux	Main production application containers within Kubernetes.

Third-Party Software	
Software	**Purpose**
Microsoft Office, Google Workspace and O365	Productivity suites
Microsoft Teams, Slack and Zoom	Message and collaboration platforms
Windows Defender, McAfee and Norton360	Antivirus and security tools
Visual Studio	Version control software
GitHub	Version control software
Sublime Text	Shareware text and source code editor
Adobe Creative Cloud Suite, Sketch & Canva	Design and creative tools
WordPress, Wix and Squarespace	Website services
Auth0, Okta & AzureAD	Authentication services

Third-Party Software	
Software	**Purpose**
Azure Cognitive Services, Google Cloud AI, and IBM Watson	Cognitive services

PEOPLE

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

OneMeta's corporate structure includes the following roles:

Chief Executive Officer (CEO): The CEO is responsible for overall company strategy and execution. Guides the organization towards its mission and vision while fostering a company culture aligned with its values. Liaises with stakeholders and makes pivotal decisions for business growth.

Head Of CS & Operations: Manages customer service and oversees company operations. Ensures OneMeta satisfaction and operational efficiency. Coordinates with different departments to achieve organizational goals.

Head Of Product: Leads the product team in developing and refining products. Sets product vision and strategy and ensures alignment with company objectives. Responsible for product lifecycle and market fit.

Product Manager: Oversees specific products or product lines. Coordinates with cross-functional teams to bring products from concept to market. Analyzes market trends and makes data-driven decisions.

Product Owner Jr: Responsible for defining product features and working with development teams to execute them. Prioritizes the product backlog and ensures that the product aligns with the business objectives. Acts as a liaison between stakeholders and the product team.

Sr. Project Manager: Manages complex projects from initiation to completion. Works closely with various teams to ensure project deliverables are met on time and on budget. Oversees project risk assessments and communicates with stakeholders.

Sr. Lead Engineer: Oversees engineering teams and ensures technical excellence. Coordinates with Product and Operations to ensure seamless product development and deployment. Sets and enforces coding standards and best practices.

Solution Architect: Designs and implements complex solutions for the business. Ensures that technology architecture aligns with business needs. Works closely with engineering teams to implement solutions.

DevOps/Azure Admin: Manages CI/CD pipelines and Azure cloud infrastructure. Ensures application and infrastructure availability, scalability, and performance. Works closely with the engineering teams to automate processes.

RevOps: Manages revenue processes, data, and tools across the customer lifecycle. Optimizes sales funnels and customer retention. Coordinates with Sales, Customer Success, and Marketing to drive revenue growth.

Head of Partnerships: Responsible for forging and maintaining strategic partnerships. Coordinates with internal and external stakeholders to align partnership goals with company objectives. Manages partnership agreements and negotiations.

Head Of Sales: Leads the sales team in acquiring new customers and upselling existing ones. Develops and executes sales strategies. Manages key accounts and overseas sales metrics and forecasts.

QA Manager: Manages Quality Assurance teams to ensure product quality. Oversees testing strategies and methodologies. Works closely with Product and Engineering teams to identify issues and ensure software quality.

CTO: Oversees the technology roadmap and aligns it with business objectives. Manages software development cycles and ensures technological advancements are integrated into the business. Serves as a liaison between the technical and business sides of the organization.

DATA

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements. Customer data is captured which is utilized by OneMeta in delivering its Services.

Information takes many forms. It may be stored on computers, transmitted across networks, printed or written on paper, and spoken in conversations. All employees and contractors of OneMeta are obligated to respect and, in all cases, to protect confidential and private data. Customer information, employment-related records, and other intellectual property-related records are subject to limited exceptions, confidential as a matter of law. Many other categories of records, including company and other personnel records, and records relating to OneMeta's business and finances are, as a matter of OneMeta policy, treated as confidential. Responsibility for guaranteeing appropriate security for data, systems, and networks is shared by the OneMeta Services and IT Departments. IT is responsible for designing, implementing, and maintaining security protection and retains responsibility for ensuring compliance with the policy. In addition to management and the technology staff, individual users are responsible for the equipment and resources under his or her control.

OneMeta has policies and procedures in place to ensure prior retention and disposal of confidential and private data. The retention and data destruction policies define the retention periods and proper destruction procedures for the disposal of data. These policies are reviewed at least annually. The destruction of data is a multi-step process. OneMeta data is deleted upon termination of the contract. A ticket is created and assigned to the product team and system engineering team to coordinate the deletion of the data. First, all files received or generated from

the OneMeta are identified and deleted by the system engineering team then the product team deletes all user-related data.

Electronic communications are treated with the same level of confidentiality and security as physical documents. Networks are protected by enterprise-class firewalls and appropriate enterprise-class virus protection is in place. Password protection with assigned user rights is required for access to the network, application, and databases. Access to the network, application, and databases is restricted to authorized internal and external users of the system to prohibit unauthorized access to confidential data. Additionally, access to data is restricted to authorized applications to prevent unauthorized access outside the boundaries of the system.

PROCEDURES

Formal IT policies and procedures exist that describe logical access, computer operations, change management, incident management, and data communication standards to document the objectives for network and data security, data privacy, and integrity for both the company and its Verbum Suite and define how services should be delivered. These are communicated to employees and located within the organization's intranet.

Reviews and changes to these policies and procedures are performed annually and are approved by senior management.

Physical Security and Environmental Controls

The Company's production servers are maintained at the third-party data center and the physical security and environmental protections are the responsibility of the subservice organization. Management obtains and reviews SOC reports annually and performs periodic site visits to monitor the physical security and environmental protection controls in place at the collocation.

Logical Access

Azure handles the network, physical host, and virtual server infrastructure. OneMeta handles the administrative responsibilities involved in supporting the web, application, and database components of the platform. OneMeta has full access to log into their servers remotely using secure shell (SSH) or Windows Remote Desktop, depending on the platform. Dedicated firewalls are used to restrict administrative access to servers. Appropriate firewall rules are in place to restrict access to customer data and to limit the possibility of disruptions to customer operations from unauthorized users.

Logical access to OneMeta's networks, applications, and data is limited to properly authorized individuals. For both the OneMeta-hosted network and the OneMeta local network, logical access is controlled via standard user authentication credentials (user ID and password). No other outside access is permitted.

Change Management

For internally developed software platforms/solutions, OneMeta uses an agile-based SDLC process, which includes research and planning, analysis and design, initial development, and quality assurance (QA) testing before the final release. All software development activities follow the internal project-related business process model.

OneMeta has an Operations Security Policy in place to control information resources that require an outage for planned upgrades, maintenance, or fine-tuning. Additionally, unplanned outages may occur that may result in upgrades, maintenance, or fine-tuning. The purpose of the Change Management Policy is to manage changes rationally and predictably so that staff and OneMeta can plan accordingly. Changes require forethought, monitoring, and follow-up evaluation to reduce negative impact on the user community and to increase the value of Information Resources. The OneMeta Operations Security Policy applies to all individuals who install, operate, or maintain Information Resources.

Patch Management

OneMeta takes a proactive approach to patch management. The CTO and engineers regularly monitor various websites, message boards, and mailing lists where advanced notifications of bug-related patches are often disclosed prior to a public announcement by the vendor. This allows the company to plan for upcoming patches.

The networking team reviews the availability of patches and independently determines if it is necessary to deploy within the production environment. Approved patches are scheduled for installation in the test environment weekly as applicable. If there are no issues in the test environment after a week, the patch will be applied to the production environment. The patching process is tracked via a HubSpot ticket.

Backup and Recovery

OneMeta maintains real-time, full system replication of the production platform between the different cloud-based data centers.

In addition, OneMeta servers utilize full and incremental backups. The retention period for these jobs is specified in the company policies based on a rotation period of incremental backups and one full backup job. Jobs are run nightly on a regular schedule with schedules distributed based on server function. Emails are generated on job completion and reviews are completed daily with additional monitoring via service alerts. Weekly backup summary emails are also generated.

All backups are encrypted and stored onsite in the dedicated backup servers.

Problem Management

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

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

System Monitoring

The Network Security and Vulnerability Management Policy describes the organization's policies and procedures related to network logging and monitoring as well as vulnerability identification and remediation. The organization uses Azure Monitor for system logging within the Azure environment, and the organization collects logs from the router and firewall. logs and the firewall logs document source IP, destination IP, destination port, protocol type, and timestamp. The organization monitors system capacity use.

Intruder is used for threat detection purposes, and the tool generates logs, VPC flow logs, and DNS logs for intrusion detection.

The vulnerability assessment process involves the execution of CIS testing, implementation of antivirus software, and system patching. The organization uses standard and up-to-date antivirus and has configured the software to run updates daily and prohibit end-users from disabling or altering the software. Alerts are sent immediately when a potential virus is detected, and logs are generated and retained for at least one year with at least three months readily available. Intruder is used to identify newly emerging vulnerabilities, and the organization monitors vendors for patch updates to correct vulnerabilities.

Incident Management

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

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

Vendor Management

The organization maintains a Vendor Management Policy that includes requirements for interacting with vendors/service providers. The policy includes requirements for performing due diligence measures prior to engaging with a new provider. Due diligence procedures include evaluating each material IT vendor's cost-effectiveness, functionality/services, risk, financial viability, compliance, and performance. The organization is required to define service levels when negotiating an arrangement with a new vendor or re-negotiating an existing arrangement, and all service levels are agreed upon and documented clearly. The organization monitors its providers' service levels to ensure each provider is providing the agreed-upon services and is compliant with all requirements. The organization executes non-disclosure agreements with third parties before any information is shared.

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

CONTROL ENVIRONMENT

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

Management Philosophy, Integrity, and Ethical Values

OneMeta's control environment reflects the philosophy of senior management concerning the importance of the security of data. Integrity and ethical values are essential elements of OneMeta's control environment. Management is responsible for setting the tone at the top, establishing, communicating, and monitoring control policies and procedures.

Formal policies, code of conduct, and employee handbooks are documented and communicated to employees to ensure that entity values, ethics, integrity, and behavioral standards are a primary focus, and risks are mitigated in daily operations. In addition, a sanctions policy is in place to address deviations from established security and personnel standards.

Management's philosophy and operating style affect the way the entity is managed, including the kinds of business risks accepted. OneMeta places a great deal of importance on working to ensure that the integrity of processing is a primary focus and that controls are maximized to mitigate risk in daily operations. Management and specific teams are structured to ensure the highest level of integrity and efficiency in customer support and transaction processing.

Formal job descriptions, departmental meetings and staff interactions ensure communication of organizational values, ethics, and behavior standards. Personnel operates under OneMeta's policies and procedures, including confidentiality agreements and security policies. Annual training is conducted to communicate regulations and the importance of privacy and security. Management is committed to being aware of regulatory and economic changes that impact lines of business and monitoring the customer base for trends, changes, and anomalies.

Commitment to Competence

OneMeta has standardized human resource policies and procedures. The result is a uniform set of practices that provide equitable hiring and advancement opportunities across the organization.

Training and development opportunities are provided to staff and performance evaluations are performed to communicate goals based on job responsibilities and address any performance issues.

Employees are trained in their specific roles and policies through on-the-job training and procedures are reviewed. Management communicates any changes to these policies on an ongoing basis and policies are updated as needed. In order to protect confidential internal and

OneMeta information employees are prohibited from divulging any information regarding OneMeta affairs or taking action, not in the interests of the OneMeta or the Verbum Suite.

Human Resources Policies and Procedures

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

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

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

RISK ASSESSMENT PROCESS

OneMeta regularly reviews the risks that may threaten the achievement of its service commitments and system requirements related to security. The Risk assessment process is performed by management to identify and manage risks and consider possible changes in the internal and external environment to mitigate these risks. Risk mitigation activities include the prevention, mitigation, and detection of risk via the implementation of internal controls. In addition, management also transfers risk through the organization's business insurance policies.

The OneMeta management team and other members of the engineering team monitor risk on an ongoing basis using information derived from employee input, system morning, audit results, industry experience, business environment, and internal system and/or process changes.

On an annual basis, management completes a risk assessment as part of the annual risk management activities. Risks identified during the annual risk assessment process include the following:

- Operational Risk
- Strategic Risk
- Compliance Risk
- Fraud Risk
- Environmental Risk

CONTROL ACTIVITIES

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

INFORMATION AND COMMUNICATION SYSTEMS

OneMeta has an information security policy to help ensure that employees understand their roles and responsibilities concerning processing and controls to ensure significant events are communicated in a timely manner. These include formal and informal training programs and the use of email to communicate time-sensitive information and processes for security, confidentiality, and availability purposes that notify the key personnel in the event of problems.

Additional communication methods include department meetings to communicate company policies, procedures, industry or business issues, or other topics management deems key to the achievement of the organization's objectives. Communication is encouraged at all levels to promote the operating efficiency of OneMeta.

OneMeta also updates their website on an ongoing basis to inform customers and other external parties of company and industry-related issues that could affect their services and what steps the company is taking to reduce or avoid the impact to their operations. The organization's security commitments regarding the services system are included in the services agreement.

MONITORING CONTROLS

In addition to daily oversight and vulnerability assessments, management uses monitoring software to monitor the security and availability of their systems. Ongoing monitoring of internal controls is also performed by management.

Monitoring of the Subservice Organization

OneMeta uses a subservice organization to provide hosting services.

Management of OneMeta receives and reviews the SOC 2 report of Azure on an annual basis. In addition, through its daily operational activities, the management of OneMeta monitors the services performed by Azure to ensure that operations and controls expected to be implemented at the subservice organization are functioning effectively.

CHANGES TO THE SYSTEM DURING THE PERIOD

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

SYSTEM INCIDENTS DURING THE PERIOD

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

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS (CSOCs)

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

#	Complementary Subservice Organization Controls (CSOC)	Related Criteria
1	Azure is responsible for maintaining physical security and environmental protection controls over the data centers hosting the OneMeta infrastructure.	CC6.4
2	Azure is responsible for the destruction of physical assets hosting the production environment.	CC6.5

COMPLEMENTARY USER ENTITY CONTROLS (CUECs)

The OneMeta'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.

TRUST SERVICES CATEGORY, CRITERIA, AND RELATED CONTROLS

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

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

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

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

This SOC 2 Type 2 report was prepared in accordance with the AICPA attestation standards and has been performed to examine the suitability of the design and operating effectiveness of controls to meet the criteria for the Security category set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*With Revised Points of Focus—2022)* in AICPA*, Trust Services Criteria* throughout the period August 1, 2024, to October 31, 2024.

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

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

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

Footnotes for Test Results When No Tests of Operating Effectiveness Were Performed

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

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.1 – COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	The company has an approved Code of Conduct that is reviewed annually and updated as needed. Sanction policies are documented within the information security policies and procedures.	Inspected the company's Code of Conduct to determine that the company had an approved Code of Conduct that is reviewed annually and updated as needed.	No exceptions noted.
		Inspected the company's Code of Conduct to determine that sanction policies were documented within the information security policies and procedures.	No exceptions noted.
CC1.1.2	The company requires employees and contractors to acknowledge the Code of Conduct at the time of hire and active employees and contractors to acknowledge the Code of Conduct at least annually.	Inspected the Code of Conduct acknowledgment for a sample of new employees and contractors to determine that the Code of Conduct was acknowledged at the time of hire.	No exceptions noted.
		Per inquiry with management and inspection of the Code of Conduct acknowledgment records for active employees and contractors, it was noted that the acknowledgments were performed in June 2024; therefore, no testing was performed.	No testing performed. See footnote 2 above.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.1.3	The company requires employees to review and acknowledge the information security policies at the time of hire, active employees, and contractors to acknowledge the information security policies at least annually.	Inspected the information security policies acknowledgment for a sample of new employees and contractors to determine that the information security policies were acknowledged at the time of hire.	No exceptions noted.
		Per inquiry with management and inspection of the information security policies acknowledgment records for active employees and contractors, it was noted that the acknowledgments were performed in June 2024; therefore, no testing was performed.	No testing performed. See footnote 2 above.
CC1.1.4	The company's managers are required to complete performance evaluations for direct reports at least annually.	Per inquiry with management and inspection of the supporting documentation, there were no active employees who were subject to performance evaluations during the examination period; therefore, no testing was performed for this control.	No testing performed. See footnote 1 above.
CC1.1.5	The company performs background checks for new employees and contractors as part of its hiring process.	Inspected the background check documentation for a sample of new employees and contractors to determine whether the company conducted these checks as part of the hiring process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.1.6	Employees are required to review and acknowledge the confidentiality agreement at the time of hire.	Inspected the confidentiality agreements in the information security policies for a sample of new employees to determine that employees were required to review and acknowledge the confidentiality agreement at the time of hire.	No exceptions noted.
CC1.2 – COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2.1	The company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls.	Inspected the board members' profiles to determine that the company's board members had sufficient expertise to oversee management's ability to design, implement and operate information security controls.	No exceptions noted.
CC1.2.2	The company's board of directors meets annually and maintains formal meeting minutes.	Per inspection of the most recent board of directors meeting minutes, and inquiry with management, the annual board meeting was conducted in June 2024; therefore, no testing was performed.	No testing performed. See footnote 2 above.
CC1.2.3	The company's board of directors has a documented board charter that outlines its oversight responsibilities for internal control.	Inspected the company's internal board charter to determine that the company's board of directors had a documented charter that outlined its oversight responsibilities for internal control.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.2.4	The company's board of directors consists of members that are independent of the company.	Inspected the board of directors listing to determine that the company's board of directors consisted of members that were independent of the company.	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 company maintains an organizational chart that describes the organizational structure and reporting lines.	Inspected the company's organizational chart to determine that the company maintained an organizational chart that described the organizational structure and reporting lines.	No exceptions noted.
CC1.3.2	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Policy.	Inspected the company's Information Security Policy to determine roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in the Information Security Policy.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.3.3	The company requires employees to review and acknowledge the information security policies at the time of hire and active employees and contractors to acknowledge the information security policies at least annually.	Inspected the information security policies acknowledgment for a sample of new employees and contractors to determine that the information security policies were acknowledged at the time of hire.	No exceptions noted.
		Per inquiry with management and inspection of the information security polices acknowledgment records for active employees and contractors, it was noted that the acknowledgments were performed in June 2024; therefore, no testing was performed.	No testing performed. See footnote 2 above.
CC1.4 – COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	The company performs background checks for new employees and contractors as part of its hiring process.	Inspected the background check documentation for a sample of new employees and contractors to determine whether the company conducted these checks as part of the hiring process.	No exceptions noted.
CC1.4.2	The company's managers are required to complete performance evaluations for direct reports at least annually.	Per inquiry with management and inspection of the supporting documentation, there were no active employees who were subject to performance evaluations during the examination period; therefore, no testing was performed for this control.	No testing performed. See footnote 1 above.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.4.3	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Policy.	Inspected the company's Information Security Policy to determine roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in the Information Security Policy.	No exceptions noted.
CC1.4.4	The company requires new employees to complete security awareness training at the time of hire, active employees, and contractors to complete security training at least annually.	Inspected the security awareness training topics to determine that the security awareness training covered areas to educate personnel on information security topics and the latest trends to protect sensitive data.	No exceptions noted.
		Inspected the training records for a sample of new employees and contractors to determine that the company required employees to complete security awareness training at the time of hire.	No exceptions noted.
		Inspected the training records for a sample of active employees and contractors to determine that the company required employees and contractors to complete security awareness training annually.	Exceptions noted: The security awareness training was completed after the examination period by all active employees and contractors.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.5 – COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	The company has an approved Code of Conduct that is reviewed annually and updated as needed. Sanction policies are documented within the information security policies and procedures.	Inspected the company's Code of Conduct to determine that the company had an approved Code of Conduct.	No exceptions noted.
		Inspected the company's information security policies and procedures to determine that sanction policies were documented within the information security policies and procedures.	No exceptions noted.
CC1.5.2	The company requires employees and contractors to acknowledge the Code of Conduct at the time of hire and active employees and contractors to acknowledge the Code of Conduct at least annually.	Inspected the Code of Conduct acknowledgment for a sample of new employees and contractors to determine that the Code of Conduct was acknowledged at the time of hire.	No exceptions noted.
		Per inquiry with management and inspection of the Code of Conduct acknowledgment records for active employees and contractors, it was noted that the acknowledgments were performed in June 2024; therefore, no testing was performed.	No testing performed. See footnote 2 above.
CC1.5.3	The company's managers are required to complete performance evaluations for direct reports at least annually.	Per inquiry with management and inspection of the supporting documentation, there were no active employees who were subject to performance evaluations during the examination period; therefore, no testing was performed for this control.	No testing performed. See footnote 1 above.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.5.4	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Policy.	Inspected the company's Information Security Policy to determine roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in the Information Security Policy.	No exceptions noted.
CC1.5.5	The company requires new employees to complete security awareness training at the time of hire and active employees to complete security training at least annually.	Inspected the security awareness training topics to determine that the security awareness training covered areas to educate personnel on information security topics and the latest trends to protect sensitive data.	No exceptions noted.
		Inspected the training records for a sample of new employees to determine that the company required employees to complete security awareness training at the time of hire.	No exceptions noted.
		Inspected the training records for a sample of active employees and contractors to determine that the company required employees and contractors to complete security awareness training annually.	Exceptions noted: The security awareness training was completed after the examination period by all active employees and contractors.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
INFORMATION AND COMMUNICATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC2.1 – COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were documented and reviewed annually.	No exceptions noted.
CC2.1.2	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected the company's compliance platform to determine that control self-assessments were performed annually, and corrective actions were taken based on relevant findings.	No exceptions noted.
CC2.1.3	The company utilizes a log management tool to identify events that may potentially impact the company's ability to achieve its security objectives.	Inspected the log management tool configurations to determine that the company utilized a log management tool to identify events that may potentially impact the company's ability to achieve its security objectives.	No exceptions noted.
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	The company has security incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's Incident Response Plan and the compliance platform to determine that the company had security incident response policies and procedures that were documented and communicated to authorized users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
INFORMATION AND COMMUNICATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC2.2.2	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Policy.	Inspected the company's Information Security Policy to determine roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in the Information Security Policy.	No exceptions noted.
CC2.2.3	The company requires new employees to complete security awareness training at the time of hire and active employees to complete security training at least annually.	Inspected the security awareness training topics to determine that the security awareness training covered areas to educate personnel on information security topics and the latest trends to protect sensitive data.	No exceptions noted.
		Inspected the training records for a sample of new employees to determine that the company required employees to complete security awareness training at the time of hire.	No exceptions noted.
		Inspected the training records for a sample of active employees and contractors to determine that the company required employees and contractors to complete security awareness training annually.	Exceptions noted: The security awareness training was completed after the examination period by all active employees and contractors.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
INFORMATION AND COMMUNICATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC2.2.4	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were documented and reviewed annually.	No exceptions noted.
CC2.2.5	The company describes its products and services to internal and external users.	Inspected the company's website to determine that the company provided a description of its products and services to internal and external users.	No exceptions noted.
CC2.2.6	The company communicates system changes to authorized internal users.	Inspected an example communication to determine that the company communicated system changes to authorized internal users.	No exceptions noted.
CC2.3 – COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	The company's security commitments are communicated to customers in the Privacy Policy.	Inspected the Privacy Policy to determine that the company's security commitments were communicated to customers in the Privacy Policy.	No exceptions noted.
CC2.3.2	The company provides guidelines and technical support resources relating to system operations to customers.	Inspected the company's support page and knowledge base to determine that the company provides guidelines and technical support resources relating to system operations to customers.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
INFORMATION AND COMMUNICATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC2.3.3	The company describes its products and services to internal and external users.	Inspected the company's website to determine that the company provided a description of its products and services to internal and external users.	No exceptions noted.
CC2.3.4	The company has contact information on its website to allow users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	Inspected the company's website to determine that the company had the contact information on their website to allow users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	No exceptions noted.
CC2.3.5	The company has written agreements in place with vendors and related third parties. These agreements include security and confidentiality commitments applicable to that entity.	Inspected the Terms of Service for vendors to determine that security commitments were in place for vendors and related third parties.	No exceptions noted.
CC2.3.6	The company notifies customers of critical system changes that may affect their processing.	Inspected the company's website to determine that the company notified customers of critical system changes that may affect their processing.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC3.1 – COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the annual security risk assessment to determine that the company specified its objectives to enable the identification and assessment of risk related to the objectives.	No exceptions noted.
CC3.1.2	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the company's Risk Assessment Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC3.1.3	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC3.2 – COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC3.2.1	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the company's Risk Assessment Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC3.2.2	The company has a vendor management program in place. Components of this program include: - critical vendor inventory. - vendor's security requirements; and - annual review of critical third-party vendors and subservice organizations.	Inspected the company's Vendor Management Policy to determine that the company had a vendor management program in place that included the security requirements for vendors.	No exceptions noted.
		Inspected the vendor listing to determine that the critical vendor inventory was in place.	No exceptions noted.
		Inspected the vendor review to determine that a review of critical vendors and the subservice organization was performed annually.	Exceptions noted: The annual security review was not completed during the examination period for high/critical risk vendors.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC3.2.3	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
CC3.2.4	The company has a documented business continuity/disaster recovery (BC/DR) Plan and tests it at least annually.	Inspected the company's BC/DR Plan to determine that the company has a documented BC/DR plan.	No exceptions noted.
		Inspected the company's latest BC/DR Plan tabletop exercise meeting notes to determine that the BC/DR plan was tested annually.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC3.4 – COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
CC3.4.2	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the company's Risk Assessment Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
MONITORING ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC4.1 – COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1.1	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected the company's compliance platform to determine that control self-assessments were performed annually, and corrective actions were taken based on relevant findings.	No exceptions noted.
CC4.1.2	Vulnerability scans are performed monthly on external-facing systems. Critical and high vulnerabilities are tracked to remediation in accordance with SLAs.	Inspected a sample of completed vulnerability scan reports to determine that vulnerability scans were performed monthly on external-facing systems.	No exceptions noted.
		Per inspection of alerts generated by the Infrastructure Package and inquiry with management, no high or critical vulnerabilities were identified during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
MONITORING ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC4.1.3	The company has a vendor management program in place. Components of this program include: - critical vendor inventory. - vendor's security requirements; and - annual review of critical third-party vendors and subservice organizations.	Inspected the company's Vendor Management Policy to determine that the company had a vendor management program in place that included the security requirements for vendors.	No exceptions noted.
		Inspected the vendor listing to determine that the critical vendor inventory was in place.	No exceptions noted.
		Inspected the vendor review to determine that a review of critical vendors and the subservice organization was performed annually.	Exceptions noted: The annual security review was not completed during the examination period for high/critical risk vendors.
CC4.2 – COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
CC4.2.1	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected the company's compliance platform to determine that control self-assessments were performed annually, and corrective actions were taken based on relevant findings.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
MONITORING ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC4.2.2	The company has a vendor management program in place. Components of this program include: - critical vendor inventory. - vendor's security requirements; and - annual review of critical third-party vendors and subservice organizations.	Inspected the company's Vendor Management Policy to determine that the company had a vendor management program in place that included the security requirements for vendors.	No exceptions noted.
		Inspected the vendor listing to determine that the critical vendor inventory was in place.	No exceptions noted.
		Inspected the vendor review to determine that a review of critical vendors and the subservice organization was performed annually.	Exceptions noted: The annual security review was not completed during the examination period for high/critical risk vendors.
CC4.2.3	Vulnerability scans are performed monthly on external-facing systems. Critical and high vulnerabilities are tracked to remediation in accordance with SLAs.	Inspected a sample of completed vulnerability scan reports to determine that vulnerability scans were performed monthly on external-facing systems.	No exceptions noted.
		Per inspection of alerts generated by the Infrastructure Package and inquiry with management, no high or critical vulnerabilities were identified during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC5.1 – COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC5.1.1	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the company's Risk Assessment Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC5.1.2	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were documented and reviewed annually.	No exceptions noted.
CC5.1.3	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC5.1.4	Role-based access is configured within Azure, MongoDB, and GitHub and other supporting applications to enforce segregation of duties and restrict access to confidential information.	Inspected the system configurations for Azure, MongoDB, and GitHub, and other supporting applications to determine that role-based access was configured within Azure, MongoDB, and GitHub, and other supporting applications to enforce segregation of duties and restrict access to confidential information.	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	The company's System Access Control Policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the company's System Access Control Policy to determine that the System Access Control Policy documented the requirement functions: -for adding new users, -modifying users, and/or -removing user access.	No exceptions noted.
CC5.2.2	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's Software Development Life Cycle Policy to determine that the company had a formal SDLC methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC5.2.3	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were documented and reviewed annually.	No exceptions noted.
CC5.3 – COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were documented and reviewed annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC5.3.2	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	Inspected the company's Change Management and Software Development Life Cycle policies to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.
		Inspected the change management documentation for a sample of changes to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.
CC5.3.3	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's Software Development Life Cycle Policy to determine that the company had a formal SDLC methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC5.3.4	The company has security incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's Incident Response Plan and the compliance platform to determine that the company had security incident response policies and procedures that were documented and communicated to authorized users.	No exceptions noted.
CC5.3.5	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the annual security risk assessment to determine that the company specified its objectives to enable the identification and assessment of risk related to the objectives.	No exceptions noted.
CC5.3.6	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the company's Risk Assessment Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC5.3.7	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Policy.	Inspected the company's Information Security Policy to determine roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in the Information Security Policy.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC5.3.8	The company has a vendor management program in place. Components of this program include: - critical vendor inventory. - vendor's security requirements; and - annual review of critical third-party vendors and subservice organizations.	Inspected the company's Vendor Management Policy to determine that the company had a vendor management program in place that included the security requirements for vendors.	No exceptions noted.
		Inspected the vendor listing to determine that the critical vendor inventory was in place.	No exceptions noted.
		Inspected the vendor review to determine that a review of critical vendors and the subservice organization was performed annually.	Exceptions noted: The annual security review was not completed during the examination period for high/critical risk vendors.
CC5.3.9	The company's System Access Control Policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the company's System Access Control Policy to determine that the System Access Control Policy documented the requirements for adding, modifying, and removing user access.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.1.1	The company's System Access Control Policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the company's System Access Control Policy to determine that the System Access Control Policy documented the requirements for adding, modifying, and removing user access.	No exceptions noted.
CC6.1.2	The company has a Data Classification Policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the company's Data Classification Policy to determine that the company had a Data Classification Policy in place to help ensure that confidential data was properly secured and restricted to authorized personnel.	No exceptions noted.
CC6.1.3	The company's databases housing sensitive customer data are encrypted at rest.	Inspected the encryption configurations to determine that the company databases housing sensitive customer data are encrypted at rest.	No exceptions noted.
CC6.1.4	The company restricts privileged access to encryption keys to authorized users with a business need.	Inspected the company's Encryption Policy to determine that the company restricted privileged access to encryption keys to authorized users with a business need.	No exceptions noted.
		Inspected the list of users with privileged access to encryption keys to determine that the company restricted privileged access to authorized users with a business need.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.1.5	Role-based access is configured within Azure, MongoDB, and GitHub and other supporting applications to enforce segregation of duties and restrict access to confidential information.	Inspected the system configuration for Azure, MongoDB, and GitHub, and other supporting applications to determine that role-based access was configured within Azure, MongoDB, and GitHub, and other supporting applications to enforce segregation of duties and restrict access to confidential information.	No exceptions noted.
CC6.1.6	The company restricts privileged access to the network, application, databases, and supporting cloud infrastructure to authorized users with a business need.	Inspected the list of users with privileged access to the cloud infrastructure and application to determine that the company restricted privileged access to the network, application, databases, and supporting cloud infrastructure to authorized users with a business need.	No exceptions noted.
CC6.1.7	The company restricts privileged access to the firewall to authorized users with a business need.	Inspected the list of users with privileged access to the firewall to determine that the company restricted privileged access to the firewall to authorized users with a business need.	No exceptions noted.
CC6.1.8	The firewall is configured to prevent unauthorized access to the company's network.	Inspected the firewall rules to determine that the firewall was configured to prevent unauthorized access to the company's network.	No exceptions noted.
CC6.1.9	The company ensures that user access to in-scope system components is based on job role and function.	Inspected the user access onboarding checklist and in-scope user listings for a sample of new employees to determine that the company ensured that user access to in-scope system components was based on job role and function.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.1.10	The company requires passwords for in-scope system components to be configured according to the company's policy.	Inspected the password configurations and written password policy to determine that the company required passwords for in-scope system components to be configured according to the company's policy.	No exceptions noted.
CC6.1.11	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Inspected the MFA configurations to determine that the company's production systems could only be remotely accessed by authorized employees possessing a valid MFA method.	No exceptions noted.
CC6.1.12	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the company's Infrastructure as a Service provider's TLS certificate to determine that the company's production systems could only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
CC6.1.13	The company maintains a formal inventory of production system assets.	Inspected an inventory listing of information assets to determine that the company maintained a formal inventory of production system assets.	No exceptions noted.
CC6.1.14	The company's network is segmented to prevent unauthorized access to customer data.	Inspected the firewall rules to determine that the company's network was segmented to prevent unauthorized access to customer data.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC6.2.1	The company's System Access Control Policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the company's System Access Control Policy to determine that the System Access Control Policy documented the requirements for adding, modifying, and removing user access.	No exceptions noted.
CC6.2.2	The company conducts annual access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Per inspection of the user access review, meeting notes, and inquiry with management, the company conducted the user access review in June 2024; therefore, no testing was performed.	No testing performed. See footnote 2 above.
CC6.2.3	Logical access to systems is revoked as a component of the termination process within the company's SLAs.	Inspected the user access and offboarding checklist and in-scope user listings for a sample of terminated employees and contractors to determine that logical access to systems was revoked as a component of the termination process within the company's SLAs.	Exceptions noted: Two out of two (100%) samples exceeded the seven business day SLA for the access revocation.
CC6.2.4	The company ensures that user access to in-scope system components is based on job role and function.	Inspected the user access request and in-scope user listings for a sample of new employees to determine that the company ensured that user access to in-scope system components was based on job role and function.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
CC6.3.1	The company's System Access Control Policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the company's System Access Control Policy to determine that the System Access Control Policy documented the requirements for adding, modifying, and removing user access.	No exceptions noted.
CC6.3.2	The company conducts annual access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Per inspection of the annual user access review documentation, and inquiry with management, the user access was conducted in June 2024, therefore, no testing was performed.	No testing performed. See footnote 2 above.
CC6.3.3	Logical access to systems is revoked as a component of the termination process within the company's SLAs.	Inspected the user access and offboarding checklist and in-scope user listings for a sample of terminated employees to determine that logical access to systems was revoked as a component of the termination process within the company's SLAs.	Exceptions noted: Two out of two (100%) samples exceeded the seven business day SLA for the access revocation.
CC6.3.4	The company ensures that new user access to in-scope system components is based on job role and function.	Inspected the user access request and in-scope user listings for a sample of new employees to determine that the company ensured that user access to in-scope system components was based on job role and function.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
CC6.4.1	Management contracts with Microsoft using their Microsoft Azure to provide physical access security of its production systems.	This control activity is the responsibility of the subservice organization. Refer to the Subservice Organization section above for controls managed by the subservice organization.	
CC6.5: The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
CC6.5.1	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the data retention and disposal procedures to determine that the company had formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	No exceptions noted.
CC6.5.2	The company has electronic media containing confidential information purged or destroyed in accordance with best practices.	Per inquiry with management and inspection of disposal records, it was noted that were no disposals during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.
CC6.5.3	The destruction of physical assets hosting the production environment is the responsibility of Azure.	This control activity is the responsibility of the subservice organization. Refer to the Subservice Organization section above for controls managed by the subservice organization.	

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the company's Infrastructure as a Service provider's TLS certificate to determine that the company's production systems could only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
CC6.6.2	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Inspected the MFA configurations to determine that the company's production systems could only be remotely accessed by authorized employees possessing a valid MFA method.	No exceptions noted.
CC6.6.3	The firewall is configured to prevent unauthorized access to the company's network.	Inspected the firewall rules to determine that the firewall was configured to prevent unauthorized access to the company's network.	No exceptions noted.
CC6.6.4	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the company's website and TLS certificate to determine that the company used secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	No exceptions noted.
CC6.6.5	The company uses an Intrusion Detection System (IDS) to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the IDS configurations to determine that the company used an IDS to provide continuous monitoring of the company's network and early detection of potential security breaches.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.7: The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
CC6.7.1	The company encrypts portable and removable media devices when used.	Inspected the company's Encryption Policy to determine that the company encrypted portable and removable media devices when used.	No exceptions noted.
		Inspected the encryption configurations for a sample of devices to determine that the company encrypted portable media devices when used.	No exceptions noted.
CC6.7.2	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the company's website and TLS certificate to determine that the company used secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	No exceptions noted.
CC6.7.3	The company has a mobile device monitoring system in place to centrally monitor mobile devices supporting the service.	Inspected the company's mobile device monitoring system to determine that the company had a mobile device monitoring system in place to centrally monitor mobile devices supporting the service.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC6.8.1	The company deploys anti-malware technology to environments commonly susceptible to malicious attacks. The anti-malware software is configured to scan workstations daily and install updates as new updates/signatures are available.	Inspected the anti-malware configurations for a sample of workstations to determine that the company deployed anti-malware technology to environments commonly susceptible to malicious attacks.	No exceptions noted.
		Inspected the anti-malware configurations for a sample of workstations to determine that the anti-malware software was configured to scan workstations daily and install updates as new updates/signatures were available.	No exceptions noted.
CC6.8.2	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's Software Development Life Cycle Policy to determine that the company had a formal SDLC methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
CC7.1.1	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	Inspected the company's Change Management and Software Development Life Cycle policies to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.
		Inspected the change management documentation for a sample of changes to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.1.2	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
CC7.1.3	Vulnerability scans are performed monthly on external-facing systems. Critical and high vulnerabilities are tracked to remediation in accordance with SLAs.	Inspected a sample of completed vulnerability scan reports to determine that vulnerability scans were performed monthly on external-facing systems.	No exceptions noted.
		Per inspection of alerts generated by the Infrastructure Package and inquiry with management, no high or critical vulnerabilities were identified during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.
CC7.1.4	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected the company's Asset Management Policy to determine that the company had a configuration management procedure in place to ensure that system configurations were deployed consistently throughout the environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.1.5	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Inspected the company's Vulnerability Management Policy to determine that the company's formal policies outlined the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	No exceptions noted.
CC7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC7.2.1	The company uses an Intrusion Detection System (IDS) to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the IDS configurations to determine that the company used an IDS to provide continuous monitoring of the company's network and early detection of potential security breaches.	No exceptions noted.
CC7.2.2	The company utilizes a log management tool to identify events that may potentially impact the company's ability to achieve its security objectives.	Inspected the log management tool configurations to determine that the company utilized a log management tool to identify events that may potentially impact the company's ability to achieve its security objectives.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.2.3	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Inspected the company's Vulnerability Management Policy to determine that the company's formal policies outlined the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	No exceptions noted.
CC7.2.4	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Inspected the monitoring tool configurations to determine that an infrastructure monitoring tool was utilized to monitor systems, infrastructure, and performance and generated alerts when specific predefined thresholds were met.	No exceptions noted.
CC7.2.5	Vulnerability scans are performed monthly on external-facing systems. Critical and high vulnerabilities are tracked to remediation in accordance with SLAs.	Inspected a sample of completed vulnerability scan reports to determine that vulnerability scans were performed monthly on external-facing systems.	No exceptions noted.
		Per inspection of alerts generated by the Infrastructure Package and inquiry with management, no high or critical vulnerabilities were identified during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.2.6	Security incidents are reported to the IT personnel and tracked through to resolution in a ticketing system.	Per inquiry with management and inspection of the security incident log, we determined there were no incidents reported during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.
CC7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.3.1	The company has security incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's Incident Response Plan and the compliance platform to determine that the company had security incident response policies and procedures that were documented and communicated to authorized users.	No exceptions noted.
CC7.3.2	The company's security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the company's Incident Response Plan to determine that the company's security incidents were logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
		Per inquiry with management and inspection of the security incident log, we determined there were no incidents reported during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.4: The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.4.1	The company has security incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's Incident Response Plan and the compliance platform to determine that the company had security incident response policies and procedures that were documented and communicated to authorized users.	No exceptions noted.
CC7.4.2	The company's security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the company's Incident Response Plan to determine that the company's security incidents were logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
		Per inquiry with management and inspection of the security incident log, we determined there were no incidents reported during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.4.3	The company has an Incident Response Plan in place and tests its Incident Response Plan at least annually.	Inspected the company's Incident Response Plan to determine that the Incident Response Plan was in place and approved by management.	No exceptions noted.
		Inspected the company's incident response plan test notes to determine that the company tests its incident response plan at least annually.	No exceptions noted.
CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	The company has security incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's Incident Response Plan and the compliance platform to determine that the company had security incident response policies and procedures that were documented and communicated to authorized users.	No exceptions noted.
CC7.5.2	The company's security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the company's Incident Response Plan to determine that the company's security incidents were logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
		Per inquiry with management and inspection of the security incident log, we determined there were no incidents reported during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.5.3	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
CC7.5.4	The company has a documented business continuity/disaster recovery (BC/DR) Plan and tests it at least annually.	Inspected the company's BC/DR Plan to determine that the company has a documented BC/DR plan.	No exceptions noted.
		Inspected the company's latest BC/DR Plan tabletop exercise meeting notes to determine that the BC/DR plan was tested annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CHANGE MANAGEMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC8.1.1	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's Software Development Life Cycle Policy to determine that the company had a formal SDLC methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.
CC8.1.2	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	Inspected the company's Change Management and Software Development Life Cycle policies to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.
		Inspected the change management documentation for a sample of changes to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CHANGE MANAGEMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC8.1.3	Segregation of duties is in place to prevent developers from pushing changes to production.	Inspected the user listing for the company's change management tool to determine that developers do not have access to the production environment.	No exceptions noted.
CC8.1.4	The company restricts access to the production environment to authorized personnel.	Inspected the users with access to production to determine that the company restricts access to the production environment to authorized personnel.	No exceptions noted.
CC8.1.5	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CHANGE MANAGEMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC8.1.6	Vulnerability scans are performed monthly on external-facing systems. Critical and high vulnerabilities are tracked to remediation in accordance with SLAs.	Inspected a sample of completed vulnerability scan reports to determine that vulnerability scans were performed monthly on external-facing systems.	No exceptions noted.
		Per inspection of alerts generated by the Infrastructure Package and inquiry with management, no high or critical vulnerabilities were identified during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK MITIGATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
CC9.1.2	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the company's Risk Assessment Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC9.2: The entity assesses and manages risks associated with vendors and business partners			
CC9.2.1	The company has written agreements in place with vendors and related third parties. These agreements include security commitments applicable to that entity.	Inspected the Terms of Service for vendors to determine that security commitments were in place for vendors and related third parties.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK MITIGATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC9.2.2	The company has a vendor management program in place. Components of this program include: - critical vendor inventory. - vendor's security requirements; and - annual review of critical third-party vendors and subservice organizations.	Inspected the company's Vendor Management Policy to determine that the company had a vendor management program in place that included the security requirements for vendors.	No exceptions noted.
		Inspected the vendor listing to determine that the critical vendor inventory was in place.	No exceptions noted.
		Inspected the vendor review to determine that a review of critical vendors and the subservice organization was performed annually.	Exceptions noted: The annual security review was not completed during the examination period for high/critical risk vendors.
CC9.2.3	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the company's Risk Assessment Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK MITIGATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC9.2.4	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.

SECTION 5: OTHER INFORMATION PROVIDED BY ONEMETA INC.

OTHER INFORMATION PROVIDED BY ONEMETA INC.

Management Response to Exception at CC1.4.4, C1.5.5, and CC2.2.3: The security awareness training was completed after the examination period by all active employees and contractors.

Response: Management confirms that security awareness training was completed by all active employees and contractors following the examination period. Additionally, formal documentation outlining user responsibilities and acceptable use policies has been published and acknowledged by all users. Although these expectations were informally communicated during the audit window, the formal documentation and attestation process were finalized shortly after the period ended.

Management Response to Exception at CC3.2.2, CC4.1.3, CC4.2.2, CC5.3.8 and CC9.2.2: The annual security review was not completed during the examination period for high/critical-risk vendors.

Response: Management acknowledges that the annual security review for high and critical-risk vendors was not completed during the examination period. A formal risk assessment process is established and was executed shortly after the audit window, including identification of relevant threats, evaluation of mitigation strategies, and executive review. While the process was in place, the timing of the most recent cycle occurred just beyond the examination period.

Management Response to Exception at CC6.2.3 and CC6.3.3: Two out of two (100%) samples exceeded the seven business day SLA for the access revocation.

Response: Management recognizes that Two out of two (100%) samples exceeded the seven-business-day SLA for access revocation. The offboarding process has been formally documented and enforced, with enhancements implemented during the audit period. Several of the cited exceptions were identified internally and resolved through ongoing internal reviews. Further improvements to the timeliness of access revocation were executed immediately following the audit period.

OneMeta believes the controls are appropriately designed and operating effectively. However, the timing of documentation and implementation in relation to the examination period limited their inclusion in this year's report. Management remains committed to continuous improvement of the control environment and expects these enhancements to be fully evidenced in future audits.