Omeda Holdings, LLC
Chicago, Illinois

System and Organization Controls Report on the Description and Tests of Operating Effectiveness of the Audience Relationship Management Application System

Controls Placed in Operation Relevant to Security, Availability, and Confidentiality

SOC 2® Type 2 Report

January 1, 2023 to December 31, 2023

This report is not to be copied or reproduced in any manner without the express written approval of Omeda Holdings, LLC and Wipfli LLP. The report, including the title page, table of contents, and sections, constitutes the entire report and should be referred to only in its entirety and not by its component parts. The report contains proprietary information and is considered confidential.

Omeda Holdings, LLC

System and Organization Controls Report on the Description and Tests of Operating Effectiveness of the Audience Relationship Management Application System

January 1, 2023 to December 31, 2023

Table of Contents

Section 1
Omeda Holdings, LLC's Assertion

Omeda Holdings, LLC’s Assertion

We have prepared the accompanying description in Section 3 titled “Description of the Audience Relationship Management Application System Provided by Omeda Holdings, LLC” (the “description”) throughout the period January 1, 2023 to December 31, 2023, 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 (*AICPA*, Description Criteria)*. The description is intended to provide report users with information about the Audience Relationship Management Application System that may be useful when assessing the risks arising from interactions with Omeda Holdings, LLC’s (“Omeda”) system, particularly information about system controls that Omeda has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (the “applicable trust services criteria”) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Omeda, to achieve Omeda’s service commitments and system requirements based on the applicable trust services criteria. The description presents Omeda’s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Omeda’s controls.

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

1. The description presents the Audience Relationship Management Application System that was designed and implemented throughout the period January 1, 2023 to December 31, 2023, in accordance with the description criteria.

2. The controls stated in the description were suitably designed throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that Omeda’s service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of Omeda’s controls throughout that period.

3. The controls stated in the description operated effectively throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that Omeda’s service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of Omeda’s controls operated effectively throughout that period.

Section 2
Independent Service Auditor’s Report

WIPFLI

Independent Service Auditor's Report

Management of Omeda Holdings, LLC
Chicago, Illinois

Scope

We have examined the accompanying description in Section 3 titled "Description of the Audience Relationship Management Application System Provided by Omeda Holdings, LLC" throughout the period January 1, 2023 to December 31, 2023 (the "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* (AICPA, *Description Criteria*) (the "description criteria"), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that Omeda Holdings, LLC's ("Omeda") service commitments and system requirements were achieved based on the trust services criteria related to security, availability, and confidentiality (the "applicable trust services criteria") set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Omeda uses a subservice organization to provide data center services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Omeda, to achieve Omeda's service commitments and system requirements based on the applicable trust services criteria. The description presents Omeda's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Omeda's controls. The description does not disclose the actual controls at the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with the controls at Omeda, to achieve Omeda's service commitments and system requirements based on the applicable trust services criteria. The description presents Omeda's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Omeda's controls. Our examination did not include such complementary user entity controls, and we have not evaluated the suitability of the design and operating effectiveness of such controls.

The information included in Section 5 titled "Other Information Provided by Omeda Holdings, LLC" is presented by management of Omeda to provide additional information and is not a part of the description. Information about Omeda's management responses has not been subjected to the procedures applied in the examination of the description and of the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria, and accordingly we express no opinion on it.

Service Organization's Responsibilities

Omeda is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Omeda's service commitments and system requirements were achieved. Omeda has provided the accompanying assertion in Section 1 titled "Omeda Holdings, LLC's Assertion" (the "assertion") about the description and the suitability of the design and operating effectiveness of controls stated therein. Omeda is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization’s service commitments and system requirements.

Service Auditor's Responsibilities

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

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

Service Auditor’s Independence and Quality Control

We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA.

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

Inherent Limitations

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

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

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

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are presented in Section 4 titled “Trust Services Categories, Criteria, and Related Controls and Independent Service Auditor’s Tests of Controls and Results” of this report.

Opinion

In our opinion, in all material respects:

- The description presents the Audience Relationship Management Application System that was designed and implemented throughout the period January 1, 2023 to December 31, 2023, in accordance with the description criteria.
- The controls stated in the description were suitably designed throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that Omeda’s service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively throughout the period and if the subservice organization and user entities applied the complementary controls assumed in the design of Omeda’s controls throughout that period.
- The controls stated in the description operated effectively throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that Omeda’s service commitments and system requirements would be achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of Omeda’s controls operated effectively throughout that period.

Restricted Use

This report, including the description of the tests of controls and results thereof in Section 4, is intended solely for the information and use of Omeda, user entities of Omeda’s Audience Relationship Management Application System during some or all of the period January 1, 2023 to December 31, 2023, business partners of Omeda subject to risks arising from interactions with the Audience Relationship Management Application System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators, all who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization’s system interacts with user entities, business partners, subservice organizations, and other parties as applicable
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization’s service commitments and system requirements

- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

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

Wipfli LLP

Wipfli LLP

Minneapolis, Minnesota
April 8, 2024

Section 3
Description of the Audience Relationship Management Application System Provided by Omeda Holdings, LLC

Description of the Audience Relationship Management Application System Provided by Omeda Holdings, LLC

Company Overview

Nature of Business

Omeda Holdings, LLC ("Omeda" or "the Company") was founded as an Illinois limited liability company. Its business is to provide companies the use of technology to segment and target their subscriber base. Over the years, as technology has advanced and client needs have evolved, Omeda's core capabilities have expanded to encompass print, email, and web-based audience solutions. Along the way, Omeda has invested in modern infrastructure to capitalize on strong processing power and to maintain the most sophisticated data-matching capabilities. Omeda remains privately owned and relationship-focused. Omeda's headquarters are located in Chicago, Illinois.

Services Provided

Omeda Holdings, LLC Audience Relationship Management System

Audience Relationship Management System™ provides a view of client data. Omeda connects data from multiple touch points including digital, events, data subscriptions, and offline data.

Omeda's focus on data quality and governance gives its clients the confidence required to make accurate and effective decisions about their customers. Customers can be segmented with standardized in-depth reporting, analytics, and insights. Through a proprietary matching algorithm, clients will receive a single view of the customer, see online and offline behaviors, and manage subscriptions more efficiently and effectively.

By connecting and integrating event data, segmenting attendees, and tailoring high-value promotions, marketing efficiency can be improved. The real-time event solution increases attendee satisfaction, booth traffic, and exhibitor revenue. Collecting this data allows greater insight into clients' online traffic, actions, and audience behaviors across multiple sites. With a small amount of JavaScript, clients can begin capturing audience behaviors, convert anonymous traffic to known traffic, and integrate web data into the Omeda Portal.

Rich, tailored premium content can be created with a simple drag-and-drop interface that integrates with the client's Content Management System (CMS). An embedded application programming interface (API) service for authenticating users, tying back to their profile to better target your customer audience, is in place.

Omeda's data can be integrated with industry-leading platforms and applications. Bidirectional APIs enable Omeda's clients to easily transfer data between enterprise platforms. Omeda provides clients the foundational elements, including hierarchies and linkage, to help ensure high-quality, dependable, and consistent data.

Omeda helps to analyze the data-driven insights about each client's audience. Business decisions are improved by leveraging data intelligence and defining data strategy and best practices, increasing knowledge of available marketing technology and identifying where and when content is being accessed, which drives new product development and creates new revenue streams for clients.

Principal Service Commitments and System Requirements

Omeda is committed to providing clients and employees a business environment that promotes ethical values, competent and timely service delivery, and clear roles and responsibilities through organizational structure, policies and procedures, and delivery on commitments to the client.

Omeda cultivates this environment by encouraging control consciousness on the part of employees. This awareness starts with executive management involvement in the creation and monitoring of policies and procedures. Sign-off by a managing executive is required for the creation or update of policies and procedures. Policies and procedures are then disseminated through the various levels of the organization. Such a control environment influences the way Omeda's business activities are structured, objectives are established, and risks are assessed.

Security, confidentiality and availability commitments to user entities are documented and communicated in contracts.

- Security commitments include limiting access to systems based on the concept of least privilege.
- Confidentiality commitments include the use of encryption technologies to protect customer data for incoming and outgoing network traffic.
- Availability commitments include the use of monitoring and environmental security controls to maintain the uptime of systems.

Omeda establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Omeda's system policies and procedures, system design documentation, and contract with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies related to how the service is designed and developed, the system is operated, the internal business systems and networks are managed, and employees are hired and trained.

Audience Relationship Management Application Systems

Critical Infrastructure

Omeda's critical server infrastructure for the Audience Relationship Management System is hosted at a third-party data center. The third-party data center operates multiple data centers that are equipped with hardware and software including servers, storage devices, and networking equipment. Omeda also uses a distributed and redundant data storage system to help ensure data availability and durability. In addition, the platform includes backup and disaster recovery solutions to help ensure data integrity in case of failures. This infrastructure enables Omeda to handle sudden spikes in traffic and usage without any interruptions in service. Omeda also maintains internal networks, window based servers for managing user access and proprietary data.

Omeda has implemented multiple layers of security controls to protect its network and infrastructure from cyber threats. These include firewalls, intrusion detection and prevention systems, and security monitoring tools. The Company also conducts regular security audits and penetration testing to identify and remediate vulnerabilities.

Software

The Audience Relationship Management System is a web-based application. Audience Relationship Management System modules are produced through a formal build process performed and managed by the development managers, except for localized developer builds for unit testing purposes. This formal build process creates production software modules for release to the hosted production environment. Source code used in the build process is retrieved from the master source code archives.

Application builds are performed according to predetermined schedules based on clients' needs and release cycle schedules. During periods of heavy development activity, builds may be produced frequently. Builds are cataloged and archived.

People

Omeda's workforce related to the Audience Relationship Management System is organized into the following functional areas.

Functional Area	Responsibilities
Senior Management	Primarily responsible for setting the strategy of the business, setting objectives for the individual teams and overall decision making.
Product Management	Creates the product strategy for the business, develops the product plan and helps prioritize the development plan to execute on the strategy.
Engineering Operations	Primarily responsible for the security, availability, and performance of the production systems. Operations actively monitors production assets.
Development	Responsible for maintaining, enhancing and creating new software that forms the core of the Omeda offering.
Testing	Tests newly developed code to ensure deployed software assets meet business and client requirements and perform as designed.
Support	Responds to and resolves client issues raised through the customer ticketing system.

Procedures

Management has developed and communicated organizational policies and procedures to employees and clients. Changes to these procedures are performed annually and authorized by senior management. These procedures cover the following key security life cycle areas:

- Data classification (data at rest, in motion, and output)
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls
- Authorization, changes to, and termination of information system access
- Monitoring of security controls
- Management of access and role

Data

Data, as defined by Omeda, is managed within the Omeda Application which includes partner account data, client data, internal operational data and transactional data.

Description of the Audience Relationship Management Application System Provided by Omeda Holdings, LLC

Omeda takes in client data from every touchpoint; from events and email to print then stores it in one easily accessible database. User records are stored under a single persistent customer ID rather than email address or phone number. A client profiles remain up to date even if someone changes job titles or contact information. Customer data flows in and out of the platform via nightly, weekly or monthly automated file drops, file sweeps and/or APIs.

Description of Information Technology

<u>Change Management</u>

Application Changes

The responsibilities of the Application Development team, led by design managers and development managers, include technical design, coding, and unit testing of new and upgraded product features. There are multiple aspects of application development activities, including the design and implementation of architecture, infrastructure, tools, and products. Application requirements are defined by the design manager and approved by the development managers.

The code is developed using the latest mix of web development software tools. Developers follow a comprehensive set of guidelines and best practices when authoring source code. Code reviews are conducted by development managers to help ensure compliance with requirements and best practices.

Changes to software and bug resolution are managed via issue and project ticketing software. This enforces control over the change process for Omeda's application. There is a written policy for entering tasks for changes to the software and bug fixes for corrections to the software. Tasks are created by design managers and development managers only. Bug fixes are created by the Development, Testing, and Implementation teams.

Application source code is stored and managed via a formal source code version control process using source code management software that is described further under Source Code Access. Omeda maintains three environments that are physically and logically separated from each other: (1) development and testing, (2) staging, and (3) production.

<u>Production Changes</u>

The production environment has been designed to optimize system performance while helping ensure the best possible security protocols. The design of the security controls and the system performance reviews are done regularly with platform experts to help ensure Omeda is using best practices.

Changes coming from the review process could include a reclassification of data, a reassessment of risk, changes in incident response and recovery plans, and a verification of responsibilities for authorizing and monitoring accesses. Changes are reviewed and communicated during regular change management meetings and/or through system alerts.

The Systems team helps ensure patches are made to the operating system regularly. Production managers check weekly to see whether there are updates to other software used in the production environment. Once identified, a schedule is set to apply the patches.

Changes to the pre-production and production environments are controlled via tickets to help ensure documentation and process control of those changes.

Control of Changes

The design and development managers meet each week to discuss the current status and assign tasks and bugs to be included in scheduled releases. Once the tasks and bugs have been scheduled, the development managers are responsible for controlling and coordinating aspects of the development process until release.

The development managers meet frequently about the development of the Audience Relationship Management System with the entire programming team. These meetings must occur at least one time each week. Minutes are maintained for development meetings.

Changes completed by the Application Development team are posted to source code management software, and testing releases are produced by development managers and put on a testing server, with the full system to the testing functions, to help ensure each task and bug has been correctly completed. Updates are approved and scheduled through the change control process.

Defect Tracking and Audit Trail

Defect tracking is done in the ticketing software. Defects can be entered into the system by Development, Testing, or Implementation team members. Each defect is evaluated, assigned to a developer, and then reassigned to testing until the defect is successfully corrected. Detailed instructions are maintained, describing how authorized team members are to add bug fixes to the ticketing software. These instructions are available to team members in a common folder accessible to those who require access to them.

The determination of the priority of the defect can be suggested by the person creating the bug fix but ultimately is agreed to or amended by the application development managers.

Source Code Access

Software source code created in the development process is stored and controlled through an industry-standard source code version control system. The software source code includes source code produced by the Application Development and Content Development teams.

Application developers retrieve copies of source code through the version control system. The system provides standard versioning mechanisms including file revision management, version labeling mechanisms, and file status indicators. To make changes to a file, the developer must “check out” the file from the version control system. When changes are complete, the application developer must “check in” the revised file. The version control system has built-in reconciliation logic to help ensure application developers don’t collide or essentially lose changes upon check-in.

Testing of Changes

A separate group at Omeda is dedicated to testing. This group controls final quality sign-off for tasks and bugs.

Tasks created in ticketing must contain details for the testing of that change. That list is put together initially by the design and development managers for tasks. The list is then amended by the Testing team.

For bugs, the Testing team outlines the steps to test, but these are generally the same steps used to re-create the bug to help ensure it is corrected.

In either case (tasks or bugs), additional care is taken by the design and development managers working with the Testing team to identify potential for collateral impacts that can be the unintended result of coding for new functionality or correcting bugs.

Prior to release, a final reproduction test is made on a hosted server setup that is a mirror image, in material aspects, of the production system. A software development item is set up to document that this last step is completed prior to release to production. As part of this step, the Testing team needs to run through the tasks and bugs in the software development management software application that are part of the release and help ensure each is functioning well.

Software Release Process

The Software Release Testing team performs testing of Omeda's software products and custom development in an environment independent from developers and development activities. Specific activities include system testing, environment testing, regression testing, release acceptance testing, and development of automated testing tools.

The software release testing process focuses on determining that product quality levels are maintained with respect to operational characteristics, performance characteristics, and system reliability. These aspects are tested and monitored against supported environments (operating systems and machine configurations) and usage scenarios based on anticipated production scenarios.

The software release testing process is synchronized with other activities through the project management tool. The testing process is applied to product releases.

Software release testing follows standardized procedures to determine that the system conforms to quality control standards prior to release. Software release testing focuses primarily on testing complete data flow throughout integration points. This includes installation, environment, and data integrity testing.

Software Build Process

Software modules are produced through a formal build process performed and managed by the development managers, except for localized developer builds for unit testing purposes. This formal build process creates production software modules for release to the hosted production environment. Source code used in the build process is retrieved from the master source code archives.

Application builds are performed according to predetermined schedules based on clients' needs and release cycle schedules. During periods of heavy development activity, builds may be produced frequently. Builds are cataloged and archived.

Employee Handbook

Omeda Holdings has implemented an employee handbook that defines the code of ethics and workforce standards. New employees are required to read and acknowledge the handbook at the time of hire. Job descriptions are maintained for employees.

Security Awareness Training

Omeda provides security awareness training to employees at least annually. Omeda provides new employees with security awareness training. An Information Systems Acceptable Use Agreement that documents employees' responsibility regarding safeguarding confidential customer information is in place.

New and Terminated User Access

Network access is limited to current employees who require access to perform their job functions. A username and password are required to access Omeda’s network. Omeda’s network passwords are required to be complex and changed regularly. New user system access is assigned based on a job function. A termination checklist is completed to help ensure system access rights are disabled at the time of termination. Omeda performs background checks on new employees at the time of hire.

Network Access

Firewall and intrusion detection system (IDS) activity is logged and reviewed by the Systems Team. A firewall is in place to help prevent unauthorized external access to Omeda’s network. Incoming and outgoing network traffic is filtered through the firewall. Logs of network administrator-level activity are reviewed. Administrative-level access to Omeda's system is restricted to authorized employees based on their job functions. Network user access reviews are performed quarterly. Logs of network administrator-level activity are reviewed. Network access is limited to current employees who require access to perform their job functions. A username and password are required to access Omeda’s network. Encryption is used for incoming and outgoing network traffic. Omeda Holdings maintains a network diagram.

Physical Security

Omeda maintains physical security controls for their office suites and internal server rooms. Physical Security Key cards are required to access Omeda’s server room and are issued to employees who require access to perform their job functions. Omeda’s internal servers and networking equipment are stored in locked server rooms.

Information Access Management

With the restriction of access being the minimum necessary to provide services, Omeda restricts access to the system to only those workforce users requiring such access to provide Omeda’s services.

Technical security controls and methods that permit access to only authorized persons include unique user IDs that enable workforce members to be individually identified and tracked (no redundant user IDs) and automatic logoff from systems of workforce users from their workstations.

Security Awareness and Training

Omeda implements training for new workforce users, as well as additional training regarding Omeda’s privacy and security controls. Omeda’s authorized users acknowledge and agree that access to an Omeda user account is enabled only upon acceptance of an obligation to comply with the protocols in the Information Security Policy and that any violation may result in termination of the user account.

Omeda takes reasonable and appropriate steps to help ensure workforce members are provided training on awareness of security policies and procedures on an ongoing basis.

Login Monitoring

Omeda implements and periodically reviews the process for controlling and monitoring login attempts to systems and reporting login discrepancies. The login process includes notification displays upon login, stating that the system must be accessed only by an authorized Omeda workforce member;

limitations on the number of unsuccessful login attempts; and system messages stating which part of the login information is correct or incorrect when there is an error. After the specific predetermined number of failed login attempts, a time period is documented before permitting further login attempts, or any further attempts are rejected until a designated Omeda workforce member has given authorization.

Subservice Organization

Omeda utilizes a third-party vendor, QTS, to assist in storing its data and providing data center services. QTS is a data center solutions provider that offers a range of services including colocation, cloud and managed hosting, hybrid IT, and connectivity solutions. QTS data centers are strategically located across North America and Europe and provide customers with a secure, scalable, and flexible infrastructure for their critical IT operations.

Omeda solicits evidence of security audits from third-party systems employed to develop and maintain Omeda’s system. If SOC 2 or equivalent reports are not available, the Security Management team and system owner review the information provided by the vendor and decide of the suitability of the vendor’s controls and practices.

Significant Changes During the Examination Period

During the audit period, January 31, 2023 to December 31, 2023 the company did not have significant changes that are relevant to the organization’s service commitments and system requirements.

Relevant Aspects of Internal Control

Control Environment

Omeda is committed to providing clients and employees a business environment that promotes ethical values, competent and timely service delivery, and clear roles and responsibilities through organizational structure, policies and procedures, and delivery on commitments to the client.

Omeda cultivates this environment by encouraging control consciousness on the part of employees. This awareness starts with executive management involvement in the creation and monitoring of policies and procedures. Sign-off by a managing executive is required for the creation or update of policies and procedures. Policies and procedures are then disseminated through the various levels of the organization. Such a control environment influences the way Omeda’s business activities are structured, objectives are established, and risks are assessed.

Information and Communication

To help align Omeda’s strategic and tactical decision-making with operating performance, management is committed to maintaining effective communication with personnel. Information comes from both inside and outside Omeda and is used to guide Omeda’s strategic and tactical decision-making as well as to measure performance. External communications originate from several sources, take on many forms (state and federal legislation, client interaction, etc.), and are distributed to a number of destinations. Omeda’s management focuses on establishing multiple formats and channels of external communications to facilitate timely and appropriate communications. Omeda’s management monitors internal and external communications on an ongoing basis to assess the effectiveness of these communications.

Risk Assessment

Omeda’s risk assessment process is its identification, analysis, and management of risks relevant to the delivery of services and protection of the client’s data. Omeda utilizes a risk assessment process to identify and manage risks that could affect its ability to provide reliable services to its clients and help ensure the protection of the clients’ data. This process requires management to identify significant risks inherent in the software development and operational environments outlined in this report.

This process has facilitated the identification of various risks inherent in Omeda’s software development and operational environment and resulted in the development and implementation of reasonable measures for the ongoing management and mitigation of these findings. The risks considered by Omeda’s management on an ongoing basis include the following:

- New industry legislation and regulations
- Changes in its operating environment
- New or modified information systems
- New technology
- Processes involving partner organizations
- External systems
- New product development
- New types of data

Control Activities

Within Omeda’s business environment, control activities include the policies and procedures that help ensure that management directives are carried out. These controls safeguard Omeda's operations and business objectives.

Monitoring

Monitoring is a critical aspect of internal control in evaluating whether controls are operating as intended and whether they are modified as appropriate for changes in conditions. Management and supervisory personnel are responsible for monitoring the quality of internal control performance as a routine part of their activities. Omeda has implemented a series of management activities to measure and assess various processes involved in servicing its client base. Monitoring solutions are also deployed to log and report on system performance and resource utilization on the network.

Availability

Omeda conducts annual server backup restores. A monitoring solution also is deployed to log and report on system performance and resource utilization on the network. A Business Continuity and Disaster Recovery Plan is in place and is reviewed annually.

Confidentiality

Employees are required to sign a confidentiality/nondisclosure agreement upon hire. Additionally, contracts that define security and confidentiality requirements are in place with critical vendors. Omeda Holdings maintains a log of confidential media pending destruction. A confidential data destruction bin is located at the Omeda's office suite.

Complementary User Entity Control Considerations

Omeda's controls were designed with the assumption that certain complementary user entity controls would be operating effectively at user entities. The controls described in this report occur at Omeda and cover only a portion of a comprehensive internal controls structure. Each user entity must address the various aspects of internal control that may be unique to its particular system. This section describes the complementary user entity controls that should be developed, placed in operation, and maintained at user entities as necessary to meet the trust services criteria stated in the description of Omeda's system. The table below identifies the criteria the complementary user entity controls relate to. User entities should determine whether adequate controls have been established to provide reasonable assurance that:

User Entity Control Consideration	Most Relevant Criteria
Access to the hosted platform is limited to authorized individuals.	CC5.2, CC6.1
User access rights to the hosted platform are reviewed regularly.	CC4.1
Devices used to access the hosted platform are protected by antivirus software and updated with patches.	CC6.8
Omeda is notified of software-related issues and enhancement requests in a timely manner.	CC5.3
Security incidents are reported in a timely manner.	CC7.1

Complementary Subservice Organization Controls

Omeda's controls related to the Audience Relationship Management Application System cover only a portion of overall internal control for each user entity of Omeda. It is not feasible for the trust services criteria related to Audience Relationship Management Application System to be achieved solely by Omeda. Therefore, each user entity's internal control must be evaluated in conjunction with Omeda'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(s) as described below.

Complementary Subservice Organization Control	Most Relevant Criteria
Subservice organization is responsible for maintaining physical security of the data center where the servers used to host the Audience Relationship Management System are located.	CC5.3
Subservice organization is responsible for documenting system availability and related security policies and procedures.	CC9.1, A1.2, A1.3
Subservice organization is responsible for providing security training to its employees on a regular basis.	CC1.1, CC1.4
Subservice organization is responsible for maintaining hiring policies and procedures, including the completion of background checks for criminal records, credit reports, and education verification.	CC1.1
Subservice organization is responsible for performing assessments to identify risks and threats that could impair the ability to meet user entity commitments.	CC3.2, CC5.1, CC3.4
Subservice organization is responsible for ensuring that the disaster recovery procedures are reviewed, updated, and tested regularly.	CC7.2, CC7.5, CC9.1, A1.3
Subservice organization is responsible for reporting incidents in a timely manner.	CC7.3
Subservice organization is responsible for ensuring electronic media that contain and store confidential information are destroyed when no longer in use.	C1.2, C1.1

Section 4
Trust Services Categories, Criteria, and Related Controls and Independent Service Auditor’s Tests of Controls and Results

Trust Services Categories, Criteria, and Related Controls and Independent Service Auditor’s Tests of Controls and Results

Objectives of the Examination

This report is intended to provide user entities of Omeda’s Audience Relationship Management Application System with information about Omeda’s controls pertaining to its Audience Relationship Management Application System and also to provide user entities with information about the operating effectiveness of the controls that were tested. This report, when combined with an understanding and assessment of the controls in place at user entities, is intended to assist user entities in understanding the controls in place at Omeda for the services being outsourced.

In addition, Wipfli LLP’s (“Wipfli”) testing of controls was restricted to the categories and related controls listed in this section of the report and was not extended to all controls described in Section 3 or to controls that may be in effect at user entities. It is each interested party’s responsibility to evaluate this information in relation to the controls in place at each user entity, and if certain complementary user entity controls are not in place at a user entity, Omeda’s controls may not compensate for such weaknesses.

The categories and description of controls are the responsibility of Omeda’s management.

Description of Testing Procedures Performed

As a part of Wipfli’s examination of Omeda’s controls, Wipfli performed a variety of tests, each of which provided the basis for understanding the framework for controls, and determined whether the controls were actually in place and operated effectively in accordance with Omeda’s description of controls throughout the period January 1, 2023 to December 31, 2023.

Wipfli’s tests of the effectiveness of controls included such tests as were considered necessary in the circumstances to evaluate whether those controls, and the extent of compliance with them, are sufficient to provide reasonable, but not absolute, assurance that the specified criteria were achieved throughout the period January 1, 2023 to December 31, 2023. Wipfli’s tests of the operational effectiveness of the controls were designed to cover a representative number of samples throughout the period January 1, 2023 to December 31, 2023, for each of the controls listed in this section, which were designed to achieve the criteria for the specified category.

In selecting particular tests of operational effectiveness, Wipfli considered:

- The nature of the items being tested.
- The types of available evidential matter.
- The assessed level of control risk.
- The expected efficiency and effectiveness of the test.

Trust Services Categories, Criteria, and Related Controls and Independent Service Auditor’s Tests of Controls and Results

The procedures performed to test operating effectiveness are listed next to each of Omeda’s respective control descriptions. Test procedures performed in connection with determining the operating effectiveness of the controls include the following:

Test Procedure	Description of Test Procedure
Corroborative Inquiry	Made inquiries of appropriate organizational personnel to obtain information or corroborating evidence regarding the control descriptions, processes, and procedures. **NOTE:** Because inquiries were performed for all controls, this test may not be listed individually for every control activity included in the control testing tables.
Observation	Witnessed the utilization of controls by organization personnel. This included, but was not limited to, viewing the functionality of system applications and automated controls, scheduling routines, and witnessing the processing of transactions.
Inspection	Read documents and reports that contain an indication of performance of the control. This included, but was not limited to, reading documents and reports to determine whether authorization was evidenced and transaction information was properly recorded and controlled and examining reconciliations and evidence of review to determine whether outstanding items were properly monitored, controlled, and resolved.
Reperformance	Independently performed the relevant control. This included, but was not limited to, comparing reconciliations with proper source documents, assessing the reasonableness of reconciling items, and recalculating mathematical solutions.

Results of Testing Performed

Test results are scored as “No exceptions noted,” or the exception is noted and described in Section 5.

The following tables describe the tests of operating effectiveness that were performed in meeting the categories noted. The categories, along with the criteria and the control descriptions, are an integral part of management’s description of their system. The control descriptions were specified by Omeda.

Trust Services Categories, Criteria, and Related Controls and Independent Service Auditor’s Tests of Controls and Results

Definition of Security, Availability, and Confidentiality Trust Services Categories

Security - The system is protected against unauthorized access, use, or modification to meet the entity's commitments and system requirements.

Availability - The system is available for operation and use to meet the entity's commitments and system requirements.

Confidentiality - Information designated as confidential is protected to meet the entity's commitments and system requirements.

Criteria, Related Controls, and Independent Auditor’s Tests of Controls and Results

CC1.0 Control Environment

Criteria Number	Control Description	Description of Testing	Results of Testing
CC1.1 - The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	Omeda has implemented an employee handbook which defines the code of ethics and workforce standards. New employees are required to read and acknowledge the handbook at the time of hire and after major changes.	Inspected the employee handbook to determine whether it defined the Company’s code of ethics and workforce standards.	No exceptions noted.
		Inspected the employee handbook acknowledgments for a sample of new employees to determine whether new employees read and acknowledged the Company's employee handbook at the time of hire.	Exceptions noted, see details in Section 5.
CC1.1.2	Omeda performs background checks on new employees at the time of hire.	Inspected the background checks for a sample of new employees to determine whether new employees screenings were completed at the time of hire.	No exceptions noted.
CC1.2 - The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2.1	Omeda has a documented organizational chart that establishes delegation of authority, segregation of duties and charges the board of directors with governance of the organization.	Inspected the organizational chart to determine whether the delegation of authority and segregation of duties were established.	No exceptions noted.
CC1.2.2	Omeda holds town hall meetings quarterly to discuss corporate strategy and guidelines.	Inspected the meeting minutes for a sample of quarters to determine whether quarterly town hall meetings were held and discussed corporate strategy and guidelines.	No exceptions noted.
CC1.3 - Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3.1	Omeda has a documented organizational chart that establishes delegation of authority, segregation of duties and charges the board of directors with governance of the organization.	Inspected the organizational chart to determine whether the delegation of authority and segregation of duties were established.	No exceptions noted.
CC1.3.2	Job descriptions are maintained for employees.	Inspected the job description for a sample of current employees to determine whether job descriptions were maintained.	No exceptions noted.

Criteria Number	Control Description	Description of Testing	Results of Testing
CC1.4 - The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	Job descriptions are maintained for employees.	Inspected the job description for a sample of current employees to determine whether job descriptions were maintained.	No exceptions noted.
CC1.4.2	Omeda performs background checks on new employees at the time of hire.	Inspected the background checks for a sample of new employees to determine whether new employees screenings were completed at the time of hire.	No exceptions noted.
CC1.4.3	Omeda provides security awareness training to employees at least annually.	Inspected security awareness training report for a sample of current employees to determine whether security awareness training was completed annually.	Exceptions noted, see details in Section 5.
CC1.4.4	Annual employee performance reviews are performed by management and include assessment and review of professional development activities.	Inspected the annual performance reviews for a sample of current employees to determine whether the reviews were performed by management and included assessment and review of professional development activities.	Exceptions noted, see details in Section 5.
CC1.4.5	Omeda provides new employees with security awareness training.	Inspected the security awareness training records for a sample of new employees to determine whether security awareness training was completed.	No exceptions noted.
CC1.5 - The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	Omeda has a documented organizational chart that establishes delegation of authority, segregation of duties and charges the board of directors with governance of the organization.	Inspected the organizational chart to determine whether the delegation of authority and segregation of duties were established.	No exceptions noted.
CC1.5.2	An Information Systems Acceptable Use Agreement that documents employees' responsibility regarding safeguarding confidential customer information is in place.	Inspected the Information Systems Acceptable Use Agreement to determine whether the agreement was in place and documented employees' responsibility regarding safeguarding confidential customer information.	No exceptions noted.

Criteria Number	Control Description	Description of Testing	Results of Testing
CC1.5.3	Employees are required to sign a confidentiality/nondisclosure agreement upon hire.	Inspected the nondisclosure agreements for a sample of new employees to determine whether agreements were signed upon hire.	No exceptions noted.
CC1.5.4	Annual employee performance reviews are performed by management and include assessment and review of professional development activities.	Inspected the annual performance reviews for a sample of current employees to determine whether the reviews were performed by management and included assessment and review of professional development activities.	Exceptions noted, see details in Section 5.
CC1.5.5	Job descriptions are maintained for employees.	Inspected the job description for a sample of current employees to determine whether job descriptions were maintained.	No exceptions noted.

CC2.0 Communication and Information

Criteria Number	Control Description	Description of Testing	Results of Testing
CC2.1 - The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	Omeda holds town hall meetings quarterly to discuss corporate strategy and guidelines.	Inspected the meeting minutes for a sample of quarters to determine whether quarterly town hall meetings were held and discussed corporate strategy and guidelines.	No exceptions noted.
CC2.1.2	Firewall and IDS activity is logged and reviewed by the Network Service team.	Inspected the firewall, IDS activity logs and email communication to determine whether logs were reviewed by the Network Service team.	No exceptions noted.
CC2.1.3	A monitoring solution has been deployed to log and report on unusual system activity on the network level.	Inspected the network monitoring logs and dashboard to determine whether a monitoring solution had been deployed to log and report unusual system activity on the network level.	No exceptions noted.
CC2.2 - The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.2.1	Omeda provides security awareness training to employees at least annually.	Inspected security awareness training report for a sample of current employees to determine whether security awareness training was completed annually.	Exceptions noted, see details in Section 5.
CC2.2.2	An Information Systems Acceptable Use Agreement that documents employees' responsibility regarding safeguarding confidential customer information is in place.	Inspected the Information Systems Acceptable Use Agreement to determine whether the agreement was in place and documented employees' responsibility regarding safeguarding confidential customer information.	No exceptions noted.
CC2.2.3	Omeda has a documented organizational chart that establishes delegation of authority, segregation of duties and charges the board of directors with governance of the organization.	Inspected the organizational chart to determine whether the delegation of authority and segregation of duties were established.	No exceptions noted.
CC2.2.4	Omeda holds town hall meetings quarterly to discuss corporate strategy and guidelines.	Inspected the meeting minutes for a sample of quarters to determine whether quarterly town hall meetings were held and discussed corporate strategy and guidelines.	No exceptions noted.

Criteria, Related Controls, and Independent Auditor’s Tests of Controls and Results

Criteria Number	Control Description	Description of Testing	Results of Testing
CC2.3 - The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	Contracts that define security and confidentiality requirements are in place with critical vendors.	Inspected the vendors contracts for a sample of critical vendors to determine whether contracts that defined security and confidentiality requirements were in place.	No exceptions noted.

Criteria, Related Controls, and Independent Auditor’s Tests of Controls and Results

CC3.0 Risk Assessment

Criteria Number	Control Description	Description of Testing	Results of Testing
CC3.1 - The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	Omeda conducts an Information Risk Assessment that identifies potential threats that would impair system security commitments and requirements, analyzes the significance of risks associated with the identified the threats, analyzes potential for fraud, and determines mitigation strategies for those risks.	Inspected the information risk assessment to determine whether it was performed annually to identify potential threats which could impair system security and confidentiality commitments and requirements.	No exceptions noted.
CC3.1.2	During the risk assessment process, changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and updates of the potential threats to system objectives are identified, and mitigation strategies are discussed.	Inspected the information risk assessment to determine whether it identified and accessed potential threats that would impair system security and confidentiality commitments.	No exceptions noted.
CC3.2 - 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	Firewall and IDS activity is logged and reviewed by the Network Service team.	Inspected the firewall, IDS activity logs and email communication to determine whether logs were reviewed by the Network Service team.	No exceptions noted.
CC3.2.2	External network vulnerability assessments are conducted periodically. Vulnerabilities identified are tracked and remediated by management.	Inspected the external vulnerability assessment report and tickets to determine whether an annual external vulnerability scan was completed and vulnerabilities identified were tracked and remediated by management.	No exceptions noted.

Criteria, Related Controls, and Independent Auditor’s Tests of Controls and Results

Criteria Number	Control Description	Description of Testing	Results of Testing
CC3.2.3	Omeda conducts an Information Risk Assessment that identifies potential threats that would impair system security commitments and requirements, analyzes the significance of risks associated with the identified the threats, analyzes potential for fraud, and determines mitigation strategies for those risks.	Inspected the information risk assessment to determine whether it was performed annually to identify potential threats which could impair system security and confidentiality commitments and requirements.	No exceptions noted.
CC3.2.4	During the risk assessment process, changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and updates of the potential threats to system objectives are identified, and mitigation strategies are discussed.	Inspected the information risk assessment to determine whether it identified and accessed potential threats that would impair system security and confidentiality commitments.	No exceptions noted.
CC3.2.5	A monitoring solution has been deployed to log and report on system performance and resource utilization on the network.	Inspected the monitoring logs and dashboards to determine whether a monitoring solution was deployed to log and report on system performance and resource utilization on the network.	No exceptions noted.
CC3.2.6	An inventory list of Omeda's assets, including workstations and servers, is maintained and updated when changes occur.	Inspected the inventory list to determine whether assets, including workstations and servers were maintained and updated when changes occurred.	No exceptions noted.
CC3.3 - The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	The Information Risk Assessment includes the assessment of risks related to fraud.	Inspected the information risk assessment to determine whether the report included risks related to fraud.	No exceptions noted.
CC3.3.2	A monitoring solution has been deployed to log and report on unusual system activity on the network level.	Inspected the network monitoring logs and dashboard to determine whether a monitoring solution had been deployed to log and report unusual system activity on the network level.	No exceptions noted.

Criteria, Related Controls, and Independent Auditor’s Tests of Controls and Results

Criteria Number	Control Description	Description of Testing	Results of Testing
CC3.3.3	An Information Systems Acceptable Use Agreement that documents employees' responsibility regarding safeguarding confidential customer information is in place.	Inspected the Information Systems Acceptable Use Agreement to determine whether the agreement was in place and documented employees' responsibility regarding safeguarding confidential customer information.	No exceptions noted.
CC3.4 - The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	During the risk assessment process, changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and updates of the potential threats to system objectives are identified, and mitigation strategies are discussed.	Inspected the information risk assessment to determine whether it identified and accessed potential threats that would impair system security and confidentiality commitments.	No exceptions noted.

CC4.0 Monitoring Activities

Criteria Number	Control Description	Description of Testing	Results of Testing
CC4.1 - 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	External network vulnerability assessments are conducted periodically. Vulnerabilities identified are tracked and remediated by management.	Inspected the external vulnerability assessment report and tickets to determine whether an annual external vulnerability scan was completed and vulnerabilities identified were tracked and remediated by management.	No exceptions noted.
CC4.1.2	Omeda holds town hall meetings quarterly to discuss corporate strategy and guidelines.	Inspected the meeting minutes for a sample of quarters to determine whether quarterly town hall meetings were held and discussed corporate strategy and guidelines.	No exceptions noted.
CC4.1.3	Network user access reviews are performed quarterly.	Inspected the user access reviews for sample of quarters to determine whether they were performed quarterly.	No exceptions noted.
CC4.1.4	An Incident Response Plan is in place and reviewed annually.	Inspected the Incident Response Plan to determine whether it was in place and reviewed annually.	No exceptions noted.
CC4.1.5	Omeda conducts annual vendor due diligence on its critical vendors.	Inspected the due diligence packets for a sample of critical vendors to determine whether vendor reviews were done annually.	No exceptions noted.
CC4.1.6	Omeda conducts penetration testing of its systems annually.	Inspected the penetrations test report to determine whether annual penetration testing was completed.	No exceptions noted.
CC4.1.7	Logs of network administrator-level activity are reviewed quarterly.	Inspected the network administrator user access review tickets for a sample of quarters to determine whether administrator-level activity were reviewed quarterly.	No exceptions noted.
CC4.2 - 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	A monitoring solution has been deployed to log and report on unusual system activity on the network level.	Inspected the network monitoring logs and dashboard to determine whether a monitoring solution had been deployed to log and report unusual system activity on the network level.	No exceptions noted.

Criteria Number	Control Description	Description of Testing	Results of Testing
CC4.2.2	A monitoring solution has been deployed to log and report on system performance and resource utilization on the network.	Inspected the monitoring logs and dashboards to determine whether a monitoring solution was deployed to log and report on system performance and resource utilization on the network.	No exceptions noted.
CC4.2.3	Help desk tickets are maintained to track and document resolution steps related to system events.	Inspected help desk tickets documentation for a sample of tickets to determine whether tickets are tracked, and resolution steps related to the system events are documented.	No exceptions noted.
CC4.2.4	An Incident Response Plan is in place and reviewed annually.	Inspected the Incident Response Plan to determine whether it was in place and reviewed annually.	No exceptions noted.
CC4.2.5	Omeda holds town hall meetings quarterly to discuss corporate strategy and guidelines.	Inspected the meeting minutes for a sample of quarters to determine whether quarterly town hall meetings were held and discussed corporate strategy and guidelines.	No exceptions noted.

Criteria, Related Controls, and Independent Auditor's Tests of Controls and Results

CC5.0 Control Activities

Criteria Number	Control Description	Description of Testing	Results of Testing
CC5.1 - The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC5.1.1	A Business Continuity and Disaster Recovery Plan is in place and is reviewed annually.	Inspected the business continuity and disaster recovery plans to determine whether it was maintained and reviewed annually.	No exceptions noted.
CC5.1.2	Omeda conducts an Information Risk Assessment that identifies potential threats that would impair system security commitments and requirements, analyzes the significance of risks associated with the identified the threats, analyzes potential for fraud, and determines mitigation strategies for those risks.	Inspected the information risk assessment to determine whether it was performed annually to identify potential threats which could impair system security and confidentiality commitments and requirements.	No exceptions noted.
CC5.2 - The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	Key cards are required to access Omeda's server room and are issued to employees who require access to perform their job functions.	Inspected the data center user list and compared it to the current employee list to determine whether key cards were issued to active employees who require them to perform their job functions.	No exceptions noted.
CC5.2.2	Network access is limited to current employees who require access to perform their job functions.	Inspected the active directory user list and compared it to the current employee list to determine whether network access was limited to current employees who required access to perform their job functions.	No exceptions noted.
CC5.2.3	An Information Systems Acceptable Use Agreement that documents employees' responsibility regarding safeguarding confidential customer information is in place.	Inspected the Information Systems Acceptable Use Agreement to determine whether the agreement was in place and documented employees' responsibility regarding safeguarding confidential customer information.	No exceptions noted.
CC5.2.4	External network vulnerability assessments are conducted periodically. Vulnerabilities identified are tracked and remediated by management.	Inspected the external vulnerability assessment report and tickets to determine whether an annual external vulnerability scan was completed and vulnerabilities identified were tracked and remediated by management.	No exceptions noted.

Criteria Number	Control Description	Description of Testing	Results of Testing
CC5.2.5	Workstations and servers are deployed in accordance with baseline configuration standards in place.	Inspected the configuration for IT assets to determine whether workstations and server are configured according to the organization standards.	No exceptions noted.
CC5.2.6	Omeda conducts penetration testing of its systems annually.	Inspected the penetrations test report to determine whether annual penetration testing was completed.	No exceptions noted.
CC5.3 - The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	Omeda has a documented software change management procedure in place.	Inspected the change management policies to determine whether software change management procedures were in place.	No exceptions noted.
CC5.3.2	Information Security policies are reviewed and approved on an annual basis by IT staff and are made available to employees.	Inspected the information security policies to determine whether the policy was reviewed and approved annually and made available to employees.	No exceptions noted.

CC6.0 Logical and Physical Access Controls

Criteria Number	Control Description	Description of Testing	Results of Testing
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	Network access is limited to current employees who require access to perform their job functions.	Inspected the active directory user list and compared it to the current employee list to determine whether network access was limited to current employees who required access to perform their job functions.	No exceptions noted.
CC6.1.2	A username and password are required to access Omeda’s network.	Inspected the active directory user list and password settings to determine whether a username and password were required to access Omeda's network.	No exceptions noted.
CC6.1.3	Omeda’s network passwords are required to be complex and changed regularly.	Inspected the password configurations to determine whether network passwords were required to be complex and changed regularly.	No exceptions noted.
CC6.1.4	A firewall is in place to help prevent unauthorized external access to Omeda’s network.	Inspected the firewall configurations and network diagram to determine a firewall was in place to help prevent unauthorized external access to Omeda’s network.	No exceptions noted.
CC6.1.5	Incoming and outgoing network traffic is filtered through the firewall.	Inspected the firewall configurations to determine whether incoming and outgoing network traffic were filtered through the firewall.	No exceptions noted.
CC6.1.6	Firewall and IDS activity is logged and reviewed by the Network Service team.	Inspected the firewall, IDS activity logs and email communication to determine whether logs were reviewed by the Network Service team.	No exceptions noted.
CC6.1.7	Remote access to Omeda's network is provisioned through an encrypted connection.	Inspected the encryption configurations to determine whether remote access to Omeda's network was provisioned through an encrypted connection.	No exceptions noted.
CC6.1.8	New user system access is assigned based on a job function.	Inspected the new user access requests tickets for a sample of new employees to determine whether they were assigned based on job functions.	No exceptions noted.

Criteria, Related Controls, and Independent Auditor's Tests of Controls and Results

Criteria Number	Control Description	Description of Testing	Results of Testing
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	New user system access is assigned based on a job function.	Inspected the new user access requests tickets for a sample of new employees to determine whether they were assigned based on job functions.	No exceptions noted.
CC6.2.2	Network user access reviews are performed quarterly.	Inspected the user access reviews for sample of quarters to determine whether they were performed quarterly.	No exceptions noted.
CC6.2.3	A termination checklist is completed to help ensure system access rights are disabled at the time of termination.	Inspected the termination checklists for a sample of terminated employees to determine whether system access was disable at the time of termination.	No exceptions noted.
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	Network access is limited to current employees who require access to perform their job functions.	Inspected the active directory user list and compared it to the current employee list to determine whether network access was limited to current employees who required access to perform their job functions.	No exceptions noted.
CC6.3.2	Network user access reviews are performed quarterly.	Inspected the user access reviews for sample of quarters to determine whether they were performed quarterly.	No exceptions noted.
CC6.3.3	A username and password are required to access Omeda's network.	Inspected the active directory user list and password settings to determine whether a username and password were required to access Omeda's network.	No exceptions noted.
CC6.3.4	New user system access is assigned based on a job function.	Inspected the new user access requests tickets for a sample of new employees to determine whether they were assigned based on job functions.	No exceptions noted.

Criteria, Related Controls, and Independent Auditor’s Tests of Controls and Results

Criteria Number	Control Description	Description of Testing	Results of Testing
CC6.3.5	Administrative-level access to the Omeda system is restricted to authorized employees based on their job functions.	Inspected the administrator account list and compared it to the current employee list to determine whether system was restricted to authorized employees based on their job function.	No exceptions noted.
CC6.3.6	A termination checklist is completed to help ensure system access rights are disabled at the time of termination.	Inspected the termination checklists for a sample of terminated employees to determine whether system access was disable at the time of termination.	No exceptions noted.
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	Key cards are required to access Omeda’s server room and are issued to employees who require access to perform their job functions.	Inspected the data center user list and compared it to the current employee list to determine whether key cards were issued to active employees who require them to perform their job functions.	No exceptions noted.
CC6.4.2	Omeda’s servers and networking equipment are stored in locked server rooms.	Inspected the server room to determine whether it was locked and contained Omeda’s servers and networking equipment.	No exceptions noted.
CC6.4.3	A termination checklist is completed to help ensure system access rights are disabled at the time of termination.	Inspected the termination checklists for a sample of terminated employees to determine whether system access was disable at the time of termination.	No exceptions noted.
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	A confidential data destruction bin is located at Omeda's office suite.	Observed the confidential destruction bin to determine whether it was kept at Omeda's office premises.	No exceptions noted.
CC6.5.2	Omeda engages a third-party vendor to assist with confidential destruction of paper material and electronic media.	Inspected the third-party agreement to determine whether Omeda engaged a third-party vendor to assist with confidential destruction of paper material and electronic media.	No exceptions noted.
CC6.5.3	A Data Destruction Policy is in place to guide the secure disposal of the Company's and customers' data.	Inspected the data destruction policy to determine whether it was maintained for guiding disposal of organization's confidential data.	No exceptions noted.

Criteria, Related Controls, and Independent Auditor’s Tests of Controls and Results

Criteria Number	Control Description	Description of Testing	Results of Testing
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	A firewall is in place to help prevent unauthorized external access to Omeda’s network.	Inspected the firewall configurations and network diagram to determine a firewall was in place to help prevent unauthorized external access to Omeda’s network.	No exceptions noted.
CC6.6.2	Firewall and IDS activity is logged and reviewed by the Network Service team.	Inspected the firewall, IDS activity logs and email communication to determine whether logs were reviewed by the Network Service team.	No exceptions noted.
CC6.6.3	A username and password are required to access Omeda’s network.	Inspected the active directory user list and password settings to determine whether a username and password were required to access Omeda's network.	No exceptions noted.
CC6.6.4	Omeda’s network passwords are required to be complex and changed regularly.	Inspected the password configurations to determine whether network passwords were required to be complex and changed regularly.	No exceptions noted.
CC6.6.5	Omeda has in place a documented remote access policy that defines the security requirements for remote access.	Inspected the remote access policy to determine whether it defined the security requirements for remote access.	No exceptions noted.
CC6.6.6	Omeda maintains a network diagram.	Inspected the network diagram to determine whether it was maintained.	No exceptions noted.
CC6.6.7	Remote access to Omeda's network is provisioned through an encrypted connection.	Inspected the encryption configurations to determine whether remote access to Omeda's network was provisioned through an encrypted connection.	No exceptions noted.
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	A firewall is in place to help prevent unauthorized external access to Omeda’s network.	Inspected the firewall configurations and network diagram to determine a firewall was in place to help prevent unauthorized external access to Omeda’s network.	No exceptions noted.
CC6.7.2	An IPS is in place to help protect Omeda's network from unauthorized external access.	Inspected the IPS dashboard to determine whether an IPS was in place to protect from unauthorized access to the organization network.	No exceptions noted.

Criteria, Related Controls, and Independent Auditor’s Tests of Controls and Results

Criteria Number	Control Description	Description of Testing	Results of Testing
CC6.7.3	Omeda maintains a network diagram.	Inspected the network diagram to determine whether it was maintained.	No exceptions noted.
CC6.7.4	Encryption is used for incoming and outgoing network traffic.	Inspected the encryption configurations to determine whether incoming and outgoing traffic was encrypted.	No exceptions noted.
CC6.7.5	Information Security policies are reviewed and approved on an annual basis by IT staff and are made available to employees.	Inspected the information security policies to determine whether the policy was reviewed and approved annually and made available to employees.	No exceptions noted.
CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC6.8.1	Antivirus software is installed on Omeda’s workstations and servers.	Inspected the antivirus configurations for a sample of workstations and servers to determine whether workstations and servers had antivirus software installed.	No exceptions noted.
CC6.8.2	An IPS is in place to help protect Omeda's network from unauthorized external access.	Inspected the IPS dashboard to determine whether an IPS was in place to protect from unauthorized access to the organization network.	No exceptions noted.
CC6.8.3	Remote access to the Omeda network is logged and retained for review as needed.	Inspected the remote access review log to determine whether remote access to the network was logged and reviewed by management.	No exceptions noted.
CC6.8.4	Remote access is encrypted using a virtual private network (VPN) connection.	Inspected the remote access policy and VPN configurations to determine whether remote access was encrypted using a VPN connection.	No exceptions noted.

Criteria, Related Controls, and Independent Auditor’s Tests of Controls and Results

CC7.0 System Operations

Criteria Number	Control Description	Description of Testing	Results of Testing
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	External network vulnerability assessments are conducted periodically. Vulnerabilities identified are tracked and remediated by management.	Inspected the external vulnerability assessment report and tickets to determine whether an annual external vulnerability scan was completed and vulnerabilities identified were tracked and remediated by management.	No exceptions noted.
CC7.1.2	A monitoring solution has been deployed to log and report on system performance and resource utilization on the network.	Inspected the monitoring logs and dashboards to determine whether a monitoring solution was deployed to log and report on system performance and resource utilization on the network.	No exceptions noted.
CC7.1.3	Omeda conducts penetration testing of its systems annually.	Inspected the penetrations test report to determine whether annual penetration testing was completed.	No exceptions noted.
CC7.1.4	An Incident Response Plan is in place and reviewed annually.	Inspected the Incident Response Plan to determine whether it was in place and reviewed annually.	No exceptions noted.
CC7.1.5	A monitoring solution has been deployed to log and report on unusual system activity on the network level.	Inspected the network monitoring logs and dashboard to determine whether a monitoring solution had been deployed to log and report unusual system activity on the network level.	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	Antivirus software is installed on Omeda’s workstations and servers.	Inspected the antivirus configurations for a sample of workstations and servers to determine whether workstations and servers had antivirus software installed.	No exceptions noted.
CC7.2.2	A monitoring solution has been deployed to log and report on system performance and resource utilization on the network.	Inspected the monitoring logs and dashboards to determine whether a monitoring solution was deployed to log and report on system performance and resource utilization on the network.	No exceptions noted.

Criteria Number	Control Description	Description of Testing	Results of Testing
CC7.2.3	Help desk tickets are maintained to track and document resolution steps related to system events.	Inspected help desk tickets documentation for a sample of tickets to determine whether tickets are tracked, and resolution steps related to the system events are documented.	No exceptions noted.
CC7.2.4	A monitoring solution has been deployed to log and report on unusual system activity on the network level.	Inspected the network monitoring logs and dashboard to determine whether a monitoring solution had been deployed to log and report unusual system activity on the network level.	No exceptions noted.
CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.3.1	An Incident Response Plan is in place and reviewed annually.	Inspected the Incident Response Plan to determine whether it was in place and reviewed annually.	No exceptions noted.
CC7.3.2	Help desk tickets are maintained to track and document resolution steps related to system events.	Inspected help desk tickets documentation for a sample of tickets to determine whether tickets are tracked, and resolution steps related to the system events are documented.	No exceptions noted.
CC7.3.3	Security incidents are identified, tracked, and resolved according to the incident response procedures.	Inspected the security Incident tracker for a sample of security incidents to determine whether incidents are tacked and resolved by management.	No exceptions noted.
CC7.4 - The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.4.1	An Incident Response Plan is in place and reviewed annually.	Inspected the Incident Response Plan to determine whether it was in place and reviewed annually.	No exceptions noted.
CC7.4.2	Security incidents are identified, tracked, and resolved according to the incident response procedures.	Inspected the security Incident tracker for a sample of security incidents to determine whether incidents are tacked and resolved by management.	No exceptions noted.
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	An Incident Response Plan is in place and reviewed annually.	Inspected the Incident Response Plan to determine whether it was in place and reviewed annually.	No exceptions noted.

Criteria, Related Controls, and Independent Auditor’s Tests of Controls and Results

Criteria Number	Control Description	Description of Testing	Results of Testing
CC7.5.2	Security incidents are identified, tracked, and resolved according to the incident response procedures.	Inspected the security Incident tracker for a sample of security incidents to determine whether incidents are tacked and resolved by management.	No exceptions noted.
CC7.5.3	A Business Continuity and Disaster Recovery Plan is in place and is reviewed annually.	Inspected the business continuity and disaster recovery plans to determine whether it was maintained and reviewed annually.	No exceptions noted.

Criteria, Related Controls, and Independent Auditor’s Tests of Controls and Results

CC8.0 Change Management

Criteria Number	Control Description	Description of Testing	Results of Testing
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	Omeda has a documented software change management procedure in place.	Inspected the change management policies to determine whether software change management procedures were in place.	No exceptions noted.
CC8.1.2	A patch management policy is in place.	Inspected the patch management policy to determine whether a patch management policy was in place.	No exceptions noted.
CC8.1.3	A patch management application is used to receive, manage, and deploy patches to the workstations.	Inspected the patch configurations for a sample of workstations to determine whether a patch management application was in place and used to receive, manage, and deploy patches to the workstations.	No exceptions noted.
CC8.1.4	External network vulnerability assessments are conducted periodically. Vulnerabilities identified are tracked and remediated by management.	Inspected the external vulnerability assessment report and tickets to determine whether an annual external vulnerability scan was completed and vulnerabilities identified were tracked and remediated by management.	No exceptions noted.
CC8.1.5	Omeda conducts penetration testing of its systems annually.	Inspected the penetrations test report to determine whether annual penetration testing was completed.	No exceptions noted.
CC8.1.6	Omeda has separate development, staging, and production environments.	Inspected Omeda’s environments screenshots to determine Omeda had separate development, staging, and production environments.	No exceptions noted.
CC8.1.7	Access to the development and production environments is restricted to individuals based on their job functions.	Inspected the list of users with access to the development and production environment and compared it to the current employee list to determine whether access to the development and production environments was restricted to individuals based on their job functions	No exceptions noted.
CC8.1.8	Requested software changes are logged and tracked in a project management system.	Inspected the list of software changes to determine whether requested software changes were logged and tracked in a project management system.	No exceptions noted.

Criteria, Related Controls, and Independent Auditor’s Tests of Controls and Results

Criteria Number	Control Description	Description of Testing	Results of Testing
CC8.1.9	Software change requests are reviewed and approved by senior management prior to being assigned to Developers.	Inspected the software change tickets for a sample of changes to determine whether software change requests were reviewed and approved by senior management prior to being assigned to Developers.	No exceptions noted.
CC8.1.10	Software changes are tested prior to being moved to production.	Inspected the software change tickets for a sample of changes to determine whether changes were tested prior to being moved to production.	No exceptions noted.
CC8.1.11	Senior management approves tested software changes and implements them into production.	Inspected the software change tickets for a sample of changes to determine whether senior management approved tested software changes and implemented them into production.	No exceptions noted.

Criteria, Related Controls, and Independent Auditor’s Tests of Controls and Results

CC9.0 Risk Mitigation

Criteria Number	Control Description	Description of Testing	Results of Testing
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	Omeda performs backups of its network daily.	Inspected the network’s server backup configurations to determine whether backups were configured to be performed daily.	No exceptions noted.
CC9.1.2	Omeda monitors that backups are successfully performed daily.	Inspected the daily backup reports for a sample of days to determine whether backups were successfully performed daily.	No exceptions noted.
		Inspected the backup configuration to determine whether backups were scheduled to be performed daily.	No exceptions noted.
CC9.1.3	A Business Continuity and Disaster Recovery Plan is in place and is reviewed annually.	Inspected the business continuity and disaster recovery plans to determine whether it was maintained and reviewed annually.	No exceptions noted.
CC9.1.4	Server backup restores are tested annually.	Inspected the server backup restoration documentation to determine whether server backup stores were tested annually.	No exceptions noted.
CC9.1.5	Omeda maintains cybersecurity insurance.	Inspected the insurance policy declaration to determine whether cybersecurity insurance was maintained.	No exceptions noted.
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	Contracts that define security and confidentiality requirements are in place with critical vendors.	Inspected the vendors contracts for a sample of critical vendors to determine whether contracts that defined security and confidentiality requirements were in place.	No exceptions noted.
CC9.2.2	Omeda conducts annual vendor due diligence on its critical vendors.	Inspected the due diligence packets for a sample of critical vendors to determine whether vendor reviews were done annually.	No exceptions noted.

Criteria, Related Controls, and Independent Auditor’s Tests of Controls and Results

Additional Information Related to Availability

Criteria Number	Control Description	Description of Testing	Results of Testing
A1.1 - The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.			
A1.1.1	Omeda conducts annual vendor due diligence on its critical vendors.	Inspected the due diligence packets for a sample of critical vendors to determine whether vendor reviews were done annually.	No exceptions noted.
A1.1.2	A monitoring solution has been deployed to log and report on system performance and resource utilization on the network.	Inspected the monitoring logs and dashboards to determine whether a monitoring solution was deployed to log and report on system performance and resource utilization on the network.	No exceptions noted.
A1.1.3	Server backup restores are tested annually.	Inspected the server backup restoration documentation to determine whether server backup stores were tested annually.	No exceptions noted.
A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.			
A1.2.1	Omeda conducts annual vendor due diligence on its critical vendors.	Inspected the due diligence packets for a sample of critical vendors to determine whether vendor reviews were done annually.	No exceptions noted.
A1.2.2	A monitoring solution has been deployed to log and report on system performance and resource utilization on the network.	Inspected the monitoring logs and dashboards to determine whether a monitoring solution was deployed to log and report on system performance and resource utilization on the network.	No exceptions noted.
A1.2.3	Server backup restores are tested annually.	Inspected the server backup restoration documentation to determine whether server backup stores were tested annually.	No exceptions noted.
A1.2.4	Omeda maintains a network diagram.	Inspected the network diagram to determine whether it was maintained.	No exceptions noted.
A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A1.3.1	Server backup restores are tested annually.	Inspected the server backup restoration documentation to determine whether server backup stores were tested annually.	No exceptions noted.

Criteria, Related Controls, and Independent Auditor’s Tests of Controls and Results

Criteria Number	Control Description	Description of Testing	Results of Testing
A1.3.2	A Business Continuity and Disaster Recovery Plan is in place and is reviewed annually.	Inspected the business continuity and disaster recovery plans to determine whether it was maintained and reviewed annually.	No exceptions noted.

Additional Information Related to Confidentiality

Criteria Number	Control Description	Description of Testing	Results of Testing
C1.1 - The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
C1.1.1	Employees are required to sign a confidentiality/nondisclosure agreement upon hire.	Inspected the nondisclosure agreements for a sample of new employees to determine whether agreements were signed upon hire.	No exceptions noted.
C1.1.2	Contracts that define security and confidentiality requirements are in place with critical vendors.	Inspected the vendors contracts for a sample of critical vendors to determine whether contracts that defined security and confidentiality requirements were in place.	No exceptions noted.
C1.1.3	A Data Destruction Policy is in place to guide the secure disposal of the Company's and customers' data.	Inspected the data destruction policy to determine whether it was maintained for guiding disposal of organization's confidential data.	No exceptions noted.
C1.1.4	Encryption is used for incoming and outgoing network traffic.	Inspected the encryption configurations to determine whether incoming and outgoing traffic was encrypted.	No exceptions noted.
C1.2 - The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			
C1.2.1	An inventory list of Omeda's assets, including workstations and servers, is maintained and updated when changes occur.	Inspected the inventory list to determine whether assets, including workstations and servers were maintained and updated when changes occurred.	No exceptions noted.
C1.2.2	A confidential data destruction bin is located at Omeda's office suite.	Observed the confidential destruction bin to determine whether it was kept at Omeda's office premises.	No exceptions noted.
C1.2.3	A Data Destruction Policy is in place to guide the secure disposal of the Company's and customers' data.	Inspected the data destruction policy to determine whether it was maintained for guiding disposal of organization's confidential data.	No exceptions noted.
C1.2.4	Omeda maintains a log of confidential media pending destruction.	Inspected the confidential media destruction log to determine whether a log was maintained to track pending confidential media destruction.	No exceptions noted.
C1.2.5	Omeda engages a third-party vendor to assist with confidential destruction of paper material and electronic media.	Inspected the third-party agreement to determine whether Omeda engaged a third-party vendor to assist with confidential destruction of paper material and electronic media.	No exceptions noted.

Section 5
Other Information Provided by Omeda Holdings, LLC

Other Information Provided by Omeda Holdings, LLC

Management's Responses to Exceptions Noted During Testing of Controls

The information included below describes the management responses provided by Omeda Holdings, LLC in response to the control findings identified in Section 4 of this document. It is presented by the management of Omeda Holdings, LLC to provide additional information and is not a part of Omeda Holdings, LLC's description of its Audience Relationship Management Application System made available to user entities throughout the period January 1, 2023 to December 31, 2023. The information provided in the management responses has not been subjected to the procedures applied in the examination of the description of the Audience Relationship Management Application System and the suitability of the design and operating effectiveness of controls to meet the trust services criteria stated in the description of the Audience Relationship Management Application System, and accordingly Wipfli LLP expresses no opinion on it.

Criteria Number	Exception Description	Management Response
CC1.1.1b	For 1 out of the 4 new hires selected for testing, the employee handbook acknowledgement was not completed at the time of hire.	Due to changes in HR leadership and related process changes, this was an oversight that has since been remedied.
CC1.4.3 CC2.2.1	For 1 out of the 34 current employees selected for testing, security awareness training was not completed.	This was an oversight, and Omeda since has changed its audit process to automatically alert both, HR and the employee's manager of any missing mandatory training assignments.
CC1.4.4 CC1.5.4	For 1 out of the 34 current employees selected for testing, an annual performance review was not completed.	During the audit year, and due to changes in HR leadership, the process of VP and C-Suite reviews was changed from written reviews to verbal 1-on-1 meetings and/or reviews by the Board, during which goals and progress are discussed and evaluated, which lead to the review in question not given in writing.