Omeda Holdings, LLC
Chicago, Illinois

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

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

SOC 2® Type 1 Report

As of December 31, 2022

Omeda Holdings, LLC

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

As of December 31, 2022

Table of Contents

Section 1 Omeda Holdings, LLC's Assertion 2
Section 2 Independent Service Auditor's Report 4
Section 3 Description of the Audience Relationship Management Application System Provided by Omeda Holdings, LLC 8
Company Overview 9
Nature of Business 9
Services Provided 9
Principal Service Commitments and System Requirements 9
Audience Relationship Management Systems 10
Description of Information Technology 11
Third-Party Service Providers 15
Relevant Aspects of Internal Control 16
Control Environment 16
Information and Communication 16
Risk Assessment 16
Control Activities 17
Monitoring 17
Definition of Security, Availability, and Confidentiality Trust Services Categories 17
Complementary User Entity Control Considerations 18
Complementary Subservice Organization Controls 18
Criteria and Related Controls for Security, Availability, and Confidentiality 20

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" as of December 31, 2022, (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 is intended to provide report users with information about the risks arising from interactions with Omeda Holdings, LLC's ("Omeda") Audience Relationship Management Application System (the "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 as of December 31, 2022, in accordance with the description criteria.

2. The controls stated in the description were suitably designed as of December 31, 2022, 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 as of that date and if the subservice organization and user entities applied the complementary controls assumed in the design of Omeda's controls and those controls operated effectively as of that date.

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" as of December 31, 2022 (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 SOC 2® Report* (AICPA, *Description Criteria*), (the "description criteria") and the suitability of the design of controls, stated in the description as of December 31, 2022, to provide reasonable assurance that Omeda Holdings, LLC's ("Omeda") 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, 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.

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 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.

WIPFLI

Service Auditor's Responsibilities
Our responsibility is to express an opinion on the description and on the suitability of design of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed 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 of controls involves:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed.
- 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 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 any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design 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.

WIPFLI

Other Matter
We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Opinion
In our opinion, in all material respects:

- The description presents Omeda's Audience Relationship Management Application System that was designed and implemented as of December 31, 2022, in accordance with the description criteria.
- The controls stated in the description were suitably designed as of December 31, 2022 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 as of that date and if the subservice organization and user entities applied the complementary controls assumed in the design of Omeda's controls and those controls operated effectively as of that date.

Restricted Use
This report is intended solely for the information and use of Omeda, user entities of Omeda's Audience Relationship Management Application System as of December 31, 2022, business partners 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, 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
- 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

Atlanta, Georgia
May 17, 2023

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 confidentiality and nondisclosure agreements.

- 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.

Audience Relationship Management Systems

Critical Infrastructure

Omeda's critical server infrastructure is hosted at third-party data centers. The Company operates multiple data centers located in diverse geographic regions to help ensure high availability and data redundancy. These data centers 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 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 staff is located in Chicago and Lincolnshire, Illinois, and is organized in the following functional areas:

Functional Area	Responsibilities
Senior Management	Primarily responsible for helping ensure Omeda meets clients' and employees' expectations.
Product Management	Overall ownership of the product direction, development, operations, and client support. Operations, Development, Testing, and Support functions report to Product Management.
Operations	Primarily responsible for the security, availability, and performance of the production systems. Operations actively monitors production assets.
Development	The core of Omeda, the Development team actively enhances and improves Omeda's service.
Testing	Dedicated to helping ensure deployed software assets meet business and client requirements and perform as designed.
Support	Monitors, receives, tracks, and remediates all client and relying party concerns and issues.

Procedures

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.

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.

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

Change Management

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 five environments that are physically and logically separated from each other: (1) development on local servers, (2) testing via a local server, (3) testing, (4) pre-production, and (5) production.

Production Changes

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 Network 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 Network Service 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

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 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 temperature monitoring 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.

Third-Party Service Providers

Omeda utilizes a third-party vendor to assist in storing its data:

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.

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

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.

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 has placed into operation 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 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

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.

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.

Complementary User Entity Control Considerations

Omeda's controls were designed with the assumption that certain complementary user entity controls would be designed and implemented 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 control objectives 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 described in 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.	CC9.1.4, A1.2.3, A1.3.1
Subservice organization is responsible for providing security training to its employees on a regular basis.	CC1.1.6., CC1.4.3, CC1.4.5

Complementary Subservice Organization Control	Most Relevant Criteria
Subservice organization is responsible for maintaining hiring policies and procedures, including the completion of background checks for criminal records, credit reports, and education verification.	CC1.1.8, CC1.1.2
Subservice organization is responsible for performing assessments to identify risks and threats that could impair the ability to meet user entity commitments.	CC3.2.3, CC5.1.2, CC3.2.4, CC3.4.1
Subservice organization is responsible for ensuring that the disaster recovery procedures are reviewed, updated, and tested regularly.	CC7.2.4, CC7.5.3, CC9.1.3, A1.3.2
Subservice organization is responsible for reporting incidents in a timely manner.	CC7.3.3
Subservice organization is responsible for ensuring electronic media that contain and store confidential information are destroyed when no longer in use.	C1.2.2, C1.1.3, C1.2.3

Criteria and Related Controls for Security, Availability, and Confidentiality

CC1.0 Control Environment

Criteria Number	Control Description
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.
CC1.1.2	The employee handbook is acknowledged annually by employees.
CC1.1.3	Omeda performs background checks on new employees at the time of hire.
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 and segregation of duties.
CC1.2.2	Omeda holds town hall meetings quarterly to discuss corporate strategy and guidelines.
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 and segregation of duties.
CC1.3.2	Job descriptions are maintained for employees.
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.
CC1.4.2	Omeda performs background checks on new employees at the time of hire.
CC1.4.3	Omeda provides security awareness training to employees at least annually.
CC1.4.4	Annual employee performance reviews are performed by management and include assessment and review of professional development activities.
CC1.4.5	Omeda provides new employees with security awareness training.
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 and segregation of duties.

Criteria Number	Control Description
CC1.5.2	An Information Systems Acceptable Use Agreement that documents employees' responsibility regarding safeguarding confidential customer information is in place.
CC1.5.3	Employees are required to sign a confidentiality/nondisclosure agreement upon hire.
CC1.5.4	Annual employee performance reviews are performed by management and include assessment and review of professional development activities.
CC1.5.5	Job descriptions are maintained for employees.

CC2.0 Communication and Information

Criteria Number	Control Description
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.
CC2.1.2	Firewall and IDS activity is logged and reviewed by the Network Service team.
CC2.1.3	A monitoring solution has been deployed to log and report on unusual system activity on the network level.
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.
CC2.2.2	An Information Systems Acceptable Use Agreement that documents employees' responsibility regarding safeguarding confidential customer information is in place.
CC2.2.3	Omeda has a documented organizational chart that establishes delegation of authority and segregation of duties.
CC2.2.4	Omeda holds town hall meetings quarterly to discuss corporate strategy and guidelines.
CC2.2.5	An Incident Response Plan is in place and reviewed annually.
CC2.2.6	Omeda maintains a network diagram.
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.

CC3.0 Risk Assessment

Criteria Number	Control Description
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.
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.
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.
CC3.2.2	External network vulnerability assessments are conducted periodically. Vulnerabilities identified are tracked and remediated by management.
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.
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.
CC3.2.5	A monitoring solution has been deployed to log and report on system performance and resource utilization on the network.
CC3.2.6	An inventory list of Omeda's assets, including workstations and servers, is maintained and updated when changes occur.
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.
CC3.3.2	A monitoring solution has been deployed to log and report on unusual system activity on the network level.
CC3.3.3	An Information Systems Acceptable Use Agreement that documents employees' responsibility regarding safeguarding confidential customer information is in place.

Criteria Number	Control Description
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.

CC4.0 Monitoring Activities

Criteria Number	Control Description
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.
CC4.1.2	Omeda holds town hall meetings quarterly to discuss corporate strategy and guidelines.
CC4.1.3	Network user access reviews are performed quarterly.
CC4.1.4	An Incident Response Plan is in place and reviewed annually.
CC4.1.5	Omeda conducts annual vendor due diligence on its critical vendors.
CC4.1.6	Omeda conducts penetration testing of its systems annually.
CC4.1.7	Logs of network administrator-level activity are reviewed.
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.
CC4.2.2	A monitoring solution has been deployed to log and report on system performance and resource utilization on the network.
CC4.2.3	Help desk tickets are maintained to track and document resolution steps related to system events.
CC4.2.4	An Incident Response Plan is in place and reviewed annually.

CC5.0 Control Activities

Criteria Number	Control Description
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.
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.
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.
CC5.2.2	Network access is limited to current employees who require access to perform their job functions.
CC5.2.3	An Information Systems Acceptable Use Agreement that documents employees' responsibility regarding safeguarding confidential customer information is in place.
CC5.2.4	External network vulnerability assessments are conducted periodically. Vulnerabilities identified are tracked and remediated by management.
CC5.2.5	Workstations and servers are deployed in accordance with baseline configuration standards in place.
CC5.2.6	Omeda conducts penetration testing of its systems annually.
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.
CC5.3.2	Information Security policies are reviewed and approved on an annual basis by IT staff and are made available to employees.

CC6.0 Logical and Physical Access Controls

Criteria Number	Control Description
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.
CC6.1.2	A username and password are required to access Omeda's network.
CC6.1.3	Omeda's network passwords are required to be complex and changed regularly.
CC6.1.4	A firewall is in place to help prevent unauthorized external access to Omeda's network.
CC6.1.5	Incoming and outgoing network traffic is filtered through the firewall.
CC6.1.6	Firewall and IDS activity is logged and reviewed by the Network Service team.
CC6.1.7	Remote access to Omeda's network is provisioned through an encrypted connection.
CC6.1.8	New user system access is assigned based on a job function.
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.
CC6.2.2	Network user access reviews are performed quarterly.
CC6.2.3	A termination checklist is completed to help ensure system access rights are disabled at the time of termination.
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.
CC6.3.2	Network user access reviews are performed quarterly.
CC6.3.3	A username and password are required to access Omeda's network.

Criteria Number	Control Description
CC6.3.4	New user system access is assigned based on a job function.
CC6.3.5	Administrative-level access to the Omeda Holdings system is restricted to authorized employees based on their job functions.
CC6.3.6	A termination checklist is completed to help ensure system access rights are disabled at the time of termination.
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.
CC6.4.2	Omeda’s servers and networking equipment are stored in locked server rooms.
CC6.4.3	A termination checklist is completed to help ensure system access rights are disabled at the time of termination.
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.
CC6.5.2	Omeda engages a third-party vendor to assist with confidential destruction of paper material and electronic media.
CC6.5.3	A Data Destruction Policy is in place to guide the secure disposal of the Company's and customers' data.
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.
CC6.6.2	Firewall and IDS activity is logged and reviewed by the Network Service team.
CC6.6.3	A username and password are required to access Omeda’s network.
CC6.6.4	Omeda’s network passwords are required to be complex and changed regularly.
CC6.6.5	Omeda has in place a documented remote access policy that defines the security requirements for remote access.
CC6.6.6	Omeda maintains a network diagram.
CC6.6.7	Remote access to Omeda's network is provisioned through an encrypted connection.

Criteria Number	Control Description
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.
CC6.7.2	An IPS is in place to help protect Omeda's network from unauthorized external access.
CC6.7.3	Omeda maintains a network diagram.
CC6.7.4	Encryption is used for incoming and outgoing network traffic.
CC6.7.5	Information Security policies are reviewed and approved on an annual basis by IT staff and are made available to employees.
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.
CC6.8.2	An IPS is in place to help protect Omeda's network from unauthorized external access.
CC6.8.3	Remote access to the Omeda Holdings network is logged and retained for review as needed.
CC6.8.4	Remote access is encrypted using a virtual private network (VPN) connection.

CC7.0 System Operations

Criteria Number	Control Description
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.
CC7.1.2	A monitoring solution has been deployed to log and report on system performance and resource utilization on the network.
CC7.1.3	Omeda conducts penetration testing of its systems annually.
CC7.1.4	An Incident Response Plan is in place and reviewed annually.
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.
CC7.2.2	A monitoring solution has been deployed to log and report on system performance and resource utilization on the network.
CC7.2.3	Help desk tickets are maintained to track and document resolution steps related to system events.
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.
CC7.3.2	Help desk tickets are maintained to track and document resolution steps related to system events.
CC7.3.3	Security incidents are identified, tracked, and resolved according to the incident response procedures.
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.
CC7.4.2	Security incidents are identified, tracked, and resolved according to the incident response procedures.
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.	

Criteria Number	Control Description
CC7.5.1	An Incident Response Plan is in place and reviewed annually.
CC7.5.2	Security incidents are identified, tracked, and resolved according to the incident response procedures.
CC7.5.3	A Business Continuity and Disaster Recovery Plan is in place and is reviewed annually.

CC8.0 Change Management

Criteria Number	Control Description
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.
CC8.1.2	A patch management policy is in place.
CC8.1.3	A patch management application is used to receive, manage, and deploy patches to the workstations.
CC8.1.4	External network vulnerability assessments are conducted periodically. Vulnerabilities identified are tracked and remediated by management.
CC8.1.5	Omeda conducts penetration testing of its systems annually.
CC8.1.6	Omeda Holdings has separate development, staging, and production environments.
CC8.1.7	Access to the development and production environments is restricted to individuals based on their job functions.
CC8.1.8	Requested software changes are logged and tracked in a project management system.
CC8.1.9	Software change requests are reviewed and approved by senior management prior to being assigned to Developers.
CC8.1.10	Software changes are tested prior to being moved to production.
CC8.1.11	Senior management approves tested software changes and implements them into production.

CC9.0 Risk Mitigation

Criteria Number	Control Description
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.
CC9.1.2	Omeda monitors that backups are successfully performed daily.
CC9.1.3	A Business Continuity and Disaster Recovery Plan is in place and is reviewed annually.
CC9.1.4	Server backup restores are tested annually.
CC9.1.5	Omeda maintains cybersecurity insurance.
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.
CC9.2.2	Omeda conducts annual vendor due diligence on its critical vendors.

Additional Information Related to Availability

Criteria Number	Control Description
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.
A1.1.2	A monitoring solution has been deployed to log and report on system performance and resource utilization on the network.
A1.1.3	Server backup restores are tested annually.
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.
A1.2.2	A monitoring solution has been deployed to log and report on system performance and resource utilization on the network.
A1.2.3	Server backup restores are tested annually.
A1.2.4	Omeda maintains a network diagram.
A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.	
A1.3.1	Server backup restores are tested annually.
A1.3.2	A Business Continuity and Disaster Recovery Plan is in place and is reviewed annually.

Additional Information Related to Confidentiality

Criteria Number	Control Description
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.
C1.1.2	Contracts that define security and confidentiality requirements are in place with critical vendors.
C1.1.3	A Data Destruction Policy is in place to guide the secure disposal of the Company's and customers' data.
C1.1.4	Encryption is used for incoming and outgoing network traffic.
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.
C1.2.2	A confidential data destruction bin is located at Omeda's office suite.
C1.2.3	A Data Destruction Policy is in place to guide the secure disposal of the Company's and customers' data.
C1.2.4	Omeda Holdings maintains a log of confidential media pending destruction.