System and Organization Controls (SOC) 3 Report

Report on the Omada Identity Cloud relevant to Security and Availability

Throughout the period April 1, 2021 to March 31, 2022

Table of Contents

Independent Service Auditor's Report Provided by Laika Compliance LLC

To: Omada A/S (“Omada” or “the Company”)

Scope

We have examined Omada’s accompanying assertion titled “Assertion of Omada A/S’s Management” (assertion) that the controls within the Company’s Omada Identity Cloud (system) were effective throughout the period April 1, 2021 to March 31, 2022, to provide reasonable assurance that Omada’s service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (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 CriteService Organization’s Responsibilities

Omada 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 Omada’s service commitments and system requirements were achieved. Omada has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Omada is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor’s Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management’s assertion that controls within the system were effective throughout the period to provide reasonable assurance that the Company’s service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management’s assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization’s service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve the Company’s service commitments and system requirements based on the applicable trust services criteria.

- Performing procedures to obtain evidence about whether controls within the system were effective to achieve the Company's service commitments and system requirements based on the applicable trust services criteria.

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

Inherent Limitations

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the 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.

Opinion

In our opinion, management's assertion that Omada's controls over the Omada Identity Cloud were effective throughout the period April 1, 2021 to March 31, 2022, to provide reasonable assurance that Omada's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Laika Compliance LLC

Arlington, Virginia
May 15, 2022

Assertion of Omada A/S's Management

We, as management of Omada A/S, are responsible for:

- Identifying the Omada Identity Cloud (System) and describing the boundaries of the System, which are presented in Attachment A
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of its principal service commitments and system requirements that are the objectives of our system, which are presented in Attachment B
- Identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the principal service commitments and system requirements
- Selecting the trust services categories that are the basis of our assertion.

Omada uses a subservice organization for data center colocation services. The boundaries of the System presented in Attachment A includes only the controls of Omada and excludes controls of the subservice organization. However, the description of the boundaries of the system does present the types of controls Omada assumes have been implemented, suitably designed, and operating effectively at the subservice organization. Certain trust services criteria can be met only if the subservice organization's controls are suitably designed and operating effectively along with the related controls at Omada. However, we perform monitoring procedures for the subservice organization and based on procedures performed, nothing has been identified that prevents us from achieving our specified service commitments and system requirements.

We assert that the controls over the system were effective throughout the period April 1, 2021 to March 31, 2022, to provide reasonable assurance that Omada's service commitments and system requirements would be achieved based on the criteria relevant to Security and Availability set forth in the AICPA's TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

Very truly yours,

Omada A/S

Attachment A – Omada Identity Cloud Overview

Services Provided

Omada A/S ("Omada" or "the Company") is a software as a service company. Omada offers Identity Cloud, a software as a service cloud based identity governance and administration (IGA) solution. Omada Identity Cloud helps organizations enable and secure digital identities for all users, applications and data, while allowing organizations to provide automated access to technology assets and managing potential security and compliance risks at the same time.

INFRASTRUCTURE

The Company utilizes Microsoft Azure to provide the resources to host the Omada Identity Cloud. The Company leverages the experience and resources of Microsoft Azure to quickly and securely scale as necessary to meet current and future demand. However, the Company is responsible for designing and configuring the architecture within the cloud to ensure security and resiliency requirements are met. Controls operated by Microsoft Azure are not included in the scope of this report.

The affected criteria are included below along with the minimum controls expected to be in place at the aforementioned hosting provider:

Criteria	Complementary Subservice Organization Controls (CSOCs)
CC6.4	• Microsoft Azure is responsible for restricting data center access to authorized personnel • Microsoft Azure is responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel
CC6.5	• Microsoft Azure is responsible for securely decommissioning and physically destroying production assets in its control
CC7.2 A1.2	• Microsoft Azure is responsible for the installation of fire suppression and detection and environmental monitoring systems at the data centers • Microsoft Azure is responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS) • Microsoft Azure is responsible for overseeing the regular maintenance of environmental protections at data centers.

SOFTWARE

Software consists of the programs and software that support the Omada Identity Cloud. Software and ancillary software is used to build, support, secure, maintain, and monitor the Omada Identity Cloud.

PEOPLE

The Company develops, manages, and secures the Omada Identity Cloud via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
Executive Management (CEO/CTO)	Responsible for overseeing company-wide activities, establishing and accomplishing goals, and managing objectives.
Technical Development (Developers)	Responsible for the development, testing, deployment, and maintenance of new code for Omada Identity Cloud.
Operations	Responsible for business operations.
Sales / Marketing	Responsible for sales, content and design.

PROCEDURES

Procedures include the automated and manual procedures involved in the operation of the Omada Identity Cloud. Procedures are developed and documented by the respective teams for a variety of processes. These procedures are drafted in alignment with the overall information security policies and are updated and approved as necessary for changes in the business, but no less than annually.

The following table details the procedures as they relate to the operation of Omada Identity Cloud:

Procedure	Description
Logical and Physical Access	How the Company restricts logical and physical access, provides and removes that access, and prevents unauthorized access.
System Operations	How the Company manages the operation of the system and detects and mitigates processing deviations, including logical and physical security deviations.

Change and Configuration Management	How the Company identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
Risk and Compliance	How the entity identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.
Data Backup and Storage	How the Company manages data backups to allow for data restorations to occur if needed.
Business Continuity and Disaster Recovery (BC/DR)	How the Company identifies the steps to be taken in the event of a disaster to help resume business operations.
Data Classification and Handling	How the company classifies data included in the service and the procedures for handling the data.

DATA

Data refers to transaction streams, files, data stores, tables, and output used or processed by the Company. Through the application programming interface (API), the customer or end-user defines and controls the data they load into and store in the Omada Identity Cloud production network. Once stored in the environment, the data is accessed remotely from customer systems via the Internet.

COMPLEMENTARY USER ENTITY CONTROLS (CUECs)

Omada's controls were designed with the assumption that certain controls would be implemented by user entities (or "customers"). Certain requirements can be met only if complementary user entity controls assumed in the design of Omada's controls are suitably designed and operating effectively, along with related controls at Omada. Identified complementary user entity controls were included in the service auditor's examination of SOC 2 controls.

Attachment B – Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of Omada Identity Cloud. Customer Terms of Services include the communication of the Company's commitments to its customers.

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

The Company's principal service commitments and system requirements related to the Omada Identity Cloud include the following:

Trust Services Category	Service Commitments	System Requirements
Security	Omada will maintain the required organizational, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Data. The safeguards will include, among others, measures designed to prevent unauthorized access to, or the disclosure of, Customer Data (other than by the Customer or Users).	• Identity and access control • Security monitoring and reporting • Threat management • Security incident response • Security awareness training • Third party provider controls (vendor risk management) • Change control procedures
Availability	The Service Level Objective of Omada Identity Cloud is to achieve System Availability of Production Environments of at least 99.9% during all calendar months of the Subscription Term.	• BC/DR plan and procedures • Data backups