Report on MindManager's Cloud System Relevant to Security

SOC 3 Examination
For the Period October 16, 2022 to October 15, 2023

MindManager

Section I

Management's Assertion Provided by

MindManager

Management's Assertion Provided by MindManager

We are responsible for designing, implementing, operating, and maintaining effective controls within MindManager Cloud (MindManager) throughout the period October 16, 2022 to October 15, 2023, to provide reasonable assurance that MindManager's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period October 16, 2022 to October 15, 2023, to provide reasonable assurance that MindManager's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). MindManager's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

MindManager uses a subservice organization, to host their production environment and perform cloud computing. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at MindManager, to achieve MindManager's service commitments and system requirements based on the applicable trust services criteria. The description presents MindManager's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design MindManager's controls. The description does not disclose the actual controls at the subservice organization.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

A formalized process related to the modification of employee or contractor access was not in place and, therefore, controls were not suitably designed or operating effectively throughout the period October 16, 2022 to October 15, 2023. As a result, controls did not provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on trust services criterion 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.

Controls related to the review of the subservice organization AWS were not consistently performed and, therefore, were not operating effectively throughout the period October 16, 2022 to October 15, 2023. As a result, controls did not provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on trust services criterion CC6.4, The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

Controls related to the review of the subservice organization AWS were not consistently performed and, therefore, were not operating effectively throughout the period October 16, 2022 to October 15, 2023. As a result, controls did not provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on trust services criterion 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.

Controls related to the assessment of vendors and business partners were not consistently performed and, therefore, were not operating effectively throughout the period October 16, 2022 to October 15, 2023. As a result, controls did not provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on trust services criterion CC9.2, The entity assesses and manages risks associated with vendors and business partners.

Except for the matters in the preceding paragraph, we assert that the controls within the system were effective throughout the period October 16, 2022 to October 15, 2023, to provide reasonable assurance that MindManager's service commitments and system requirements were achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization controls assumed in the design of MindManager's controls throughout that period.

Section II

Independent Service Auditor’s Report

EideBailly

CPAs & BUSINESS ADVISORS

Independent Service Auditor's Report

To the Management of
MindManager
Austin, Texas

Scope

We have examined MindManager's accompanying assertion titled "Management's Assertion Provided by MindManager" (assertion) that the controls within MindManager Cloud (MindManager) were effective throughout the period October 16, 2022 to October 15, 2023, to provide reasonable assurance that MindManager's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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

Service Organization's Responsibilities

MindManager 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 MindManager's service commitments and system requirements were achieved. MindManager has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, MindManager 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.

345 N. Reid Pl., Ste. 400 | P.O. Box 5125 | Sioux Falls, SD 57117-5125 | T 605.339.1999 | F 605.339.1306 | EOE

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 service organization'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 qualified 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 MindManager'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 MindManager's service commitments and system requirements based the applicable trust services criteria.

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

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

Inherent Limitations

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 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.

Basis for Qualified Opinion

MindManager's system states that all requests to modify an employee's or contractor's access must be approved by management. However, as noted in Section IV of the description of tests of controls and the results thereof, a formalized process related to the modification of employee or contractor access was not in place and, therefore, controls were not suitably designed or operating effectively throughout the period October 16, 2022 to October 15, 2023. As a result, controls did not provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on trust services criterion 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.

MindManager's system states that MindManager management reviews the SOC 2 Type II examination for AWS on an annual basis to assess the potential risks related to security. However, as noted in Section IV of the description of tests of controls and the results thereof, controls related to the review of the subservice organization AWS were not consistently performed and, therefore, were not operating effectively throughout the period October 16, 2022 to October 15, 2023. As a result, controls did not provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on trust services criterion CC6.4, The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

MindManager's system states that MindManager management reviews the SOC 2 Type II examination for AWS on an annual basis to assess the potential risks related to security. However, as noted in Section IV of the description of tests of controls and the results thereof, controls related to the review of the subservice organization AWS were not consistently performed and, therefore, were not operating effectively throughout the period October 16, 2022 to October 15, 2023. As a result, controls did not provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on trust services criterion 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.

MindManager's system states that MindManager has a vetting process for screening new vendors and approving them for company use as well as rescreening vendors as necessary. However, as noted in Section IV of the description of tests of controls and the results thereof, controls related to the assessment of vendors and business partners were not consistently performed and, therefore, were not operating effectively throughout the period October 16, 2022 to October 15, 2023. As a result, controls did not provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on trust services criterion CC9.2, The entity assesses and manages risks associated with vendors and business partners.

Opinion

In our opinion, except for the effects of the matters giving rise to the modification described in the Basis for Qualified Opinion section of our report, management's assertion that the controls within MindManager Cloud relevant to security were effective throughout the period October 16, 2022 to October 15, 2023, to provide reasonable assurance that MindManager's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls assumed in the design of MindManager's controls operated effectively throughout that period.

Sioux Falls, South Dakota
February 21, 2024

Attachment A

Description of the Boundaries of the MindManager Cloud

Company Background

Since 1985 Alludo has provided technology supporting innovation to industries of all sizes and types around the world. MindManager Cloud hereafter MindManager is part of Alludo's Productivity Portfolio with a global customer base in over 200 countries and across more than 21 industries. Individuals, teams and enterprises are enabled to capture, process and share cross cutting information, transform unstructured ideas and data into dynamic visual mind maps diagrams.

MindManager controls are based on a proprietary framework of prevailing security and privacy regulations, standards and frameworks underpinned by NIST 800-53r5. These include but are not limited to: AICPA TSP 100, CCPA, CSA, GDPR, ISO/IEC 17826, ISO/IEC 27001*, ISO/IEC 27017*, ISO/IEC 27018*, ISO/IEC 27040, NIST 800-53*, NIST 800-145, NIST Cybersecurity Framework, OWASP, PIPEDA and PCI.

MindManager is a multi-cloud, multi-service, multi-tenant Software as a Service (SaaS) collaboration application deployed in a public cloud and managed through a shared responsibility model of protection with Amazon Web Services (AWS). The scope covered in this report consists of the following capabilities delivered through specific AWS services:

- Analytics
- Compute
- Containers
- Database
- Management & Governance
- Networking & Content Delivery
- Security, Identity & Compliance
- Storage

Compliance information about AWS services is found at https://aws.amazon.com/compliance/services-in-scope/

The scope of locations covered in this report includes the supporting data centers located in:

- Germany: Europe (Frankfurt) (eu-central-1)
- Ireland: Europe (Dublin) (eu-west-1)

The following AWS Edge locations and/or Local Zone are also covered in this report:

- Munich, Germany
- Dublin, Ireland

AWS is responsible for operations and security of the cloud and is the infrastructure owner. MindManager inherits security controls from the following:

Foundational

- Database
- Network
- Platform and Storage
- Physical

Cloud Orchestration

- Data
- Networking
- Operating System
- Virtualization

Infrastructure

MindManager's infrastructure is designed and managed in accordance with global security compliance standards along with industry best practices. The environments used by customers for collaboration is protected through an attack centered security control design and application of a three-tiered defense model.

The three-tiered defense model is a situational defense strategy reliant on selection, design and implementation of solutions and mechanisms design at a maximum to maintain information system availability and privacy and minimally alert should an intrusion occur. The tiers are classified below:

Three-Tiered Defense

Tier 1	Tier 2	Tier 3
• Action	• Mechanization	• Information Flow
• Preventative (stop)	• Primary	• Ingress
• Corrective (fix)	• Secondary	• Egress
• Detective (alert)	• Tertiary	

All controls associated with the three-tiered defense model align to MindManager's responsibility for operations and security of MindManager along with our role of data custodian. Controls managed and maintained by AWS are situationally inherited defined as follows:

Common Controls
Implementation provides protection for multiple information systems.

System-Specific Controls
Implementation provides protection for a specific information system.

Hybrid Controls
Implementation provides protection are both system-specific and common.

AWS capabilities and services supporting MindManager are reviewed at least annually for continuous enhancement and compliance.

Components of the System

MindManager is an information system. To us, an information system broadly is a discrete set of information resources organized for the possible collection, processing, maintenance, use, sharing, dissemination, or disposition of information. MindManager, here in after, the information system, does not process nor store customer information, rather it facilitates information use, sharing and dissemination.

Facilitation of information collaboration, also known as co-editing, is achieved across the various components defined as Sub-system(s) and Boundaries.

To us, a subsystem is a major subdivision or element of an information system consisting of information, information technology, and personnel that performs one or more specific functions as defined by NIST 800-37r2. A description of the services included within the scope of this report is listed below:

MindManager Account

Facilitates authentication and authorization of each user ensuring any data the user shares with the MindManager Cloud Services is owned, controlled and visible only to that user. It relies on a standards-based Identity Provider supporting prevailing identity and access management standards. Accounts are governed by role base access control ensuring the principle of least privilege is enforced. Accounts may be configured to support single sign-on via the customers compatible authentication provider.

MindManager License Validation

Stores customer license information for ongoing license validation with their associated product. License information is stored in a distributed, fault-tolerant, self-healing storage system supporting security, availability, and reliability. Data is protected by multiple layers of controls inclusive of: (1) network isolation (2) key management system and (3) encryption in transit using TLS 1.2.

MindManager Co-editing

Provides temporary file object storage service offering industry-leading scalability, data availability, security for customers with the appropriate license to create, open, edit, co-edit. File content is temporarily stored when there is a problem saving the MindManager file with changes from the editing session back to the original customer select permanent cloud storage location. All data stored at rest for this service is automatically deleted 7 days after the file is successfully saved back to the provider or when the user initiates deletion. The co-editing system is protected by AWS Encryption mechanisms for data at rest and in transit are industry standard and peer reviewed along with FIPS 140-2 validation. Customers utilizing co-editing are isolated using a blend of logical mechanisms inclusive of unique tenant IDs.

MindManager boundaries are transitional physical, logical and virtual resources enforcing isolation resulting in the prevention of information disclosure, theft and exfiltration of the information system. Transitional boundaries are physical, logical and virtual mechanisms when interconnected, provide access traversal throughout an information system. Boundary protection controls are defined by NIST 800-53r5.

People

MindManager's organizational structure provides a framework for planning, executing and controlling business operations. Our Executive Leadership Team and senior leadership establish the Company's tone and communicate core values. The organizational structure assigns roles and responsibilities to provide for adequate staffing, security, efficiency of operations, and segregation of duties. Management has also established authority and appropriate lines of reporting for key personnel.

The Company follows a structured on-boarding process to familiarize new employees with organizational tools, processes, privacy responsibilities, acceptable use practices, cyber security policies and procedures. Employees are provided with the Company's Code of Business Conduct and Ethics and additionally complete bi-annual Security & Awareness training for continuous awareness of threats.

Data

Customers retain ownership and control of their own data. Customers are responsible for supporting secure egress connectivity from technologies to MindManager along with ensuring their own systems and endpoints are free of malicious code and actors. MindManager is designed to prevent customers from accessing physical hosts or instances not assigned to them by disabling control mechanism associated with their unique account and tenant ID.

Threat and Vulnerability Management

At least annually, two external black-box penetration tests are performed by third parties verifying ongoing security posture has been maintained and any prior defects remediated.

Future Proofing

MindManager is committed to continuous protection of customer information and content. We maintain this commitment through a proprietary trust methodology of practices including but not limited to the following:

- Information Modeling
- Product Modeling
- Risk Modeling
- Verification

Complementary Subservice Organization Controls

MindManager's controls related to criteria listed in the table below cover only a portion of internal controls relevant to those trust services control criteria. The achievement of certain trust services criteria related to MindManager's dependency on controls, known as complementary subservice organization controls, that are performed by our subservice providers.

The technology stack of the information system is under a shared responsibility model where AWS is responsible for backup and recovery of hardware, OS and applications at the foundational layer. Back-up and redundancy of the environment is provided and managed by AWS across independent and physically separated AWS data centers. MindManager's primary site is hosted in Germany (Frankfurt) and the backup site in Ireland (Dublin).

Each user entity's internal control should be evaluated in conjunction with MindManager's controls and the related tests and results described in Section II of this report, while considering the complementary subservice organization controls expected to be implemented at the subservice organizations, as described in the table below. The scope of this report does not include criteria and controls at the external subservice organizations. Through the performance of the control activities described herein, including obtaining and evaluating available SOC reports for subservice providers, MindManager monitors subservice providers' adherence to policies and procedures.

Types of Services Provided	Subservice Organization Name	Complementary Subservice Organization Controls	Relevant Applicable Trust Services Criteria
Public Cloud Computing Platform	Amazon Web Services	Amazon Web Services is responsible for backup and recovery of the environment, physical access controls, network infrastructure, and environmental controls.	CC6.4, CC6.5

Attachment B

Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

MindManager designs its processes and procedures related to the MindManager information system to meet its objectives for its constituents. Those objectives are based on the service commitments that MindManager makes to user entities, the laws and regulations that govern the provision of MindManager Platform services, and the financial, operational, and compliance requirements that has established for the services. Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- System Uptime and Availability
- Maintenance
- Support
- Resolution of Errors
- Internal Controls and Compliance
- Hosting with AWS Cloud Computing Services
- Geographic and Physical Independence
- Business Continuity
- Network Monitoring
- Backup and Restore
- Environments
- Incident Response

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

The technology stack of the information system is under a shared responsibility model where AWS is responsible for backup and recovery of hardware, OS and applications at the foundational layer. Back-up and redundancy of the environment is provided and managed by AWS across independent and physically separated AWS data centers. MindManager's primary site is hosted in Germany (Frankfurt) and the backup site in Ireland (Dublin).