Alludo

SOC 3 Report

Corel Corporation

October 16, 2023 to October 15, 2024

An Independent Service Auditor's Report on Controls Relevant to Security

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations

AUDIT AND ATTESTATION BY

PRESCIENT ASSURANCE

CPA

Prescient Assurance LLC.
1100 Market Street Suite 600
Chattanooga, TN 37402

www.prescientassurance.com
info@prescientassurance.com
+1 646 209 7319

Table of Contents

SECTION 1

Management's Assertion

Alludo

Management Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Corel Corporation's MindManager system throughout the period October 16, 2023, to October 15, 2024, to provide reasonable assurance that Corel Corporation's service commitments and system requirements relevant to Security were achieved. 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 controls within the system throughout the period October 16, 2023, to October 15, 2024, to provide reasonable assurance that Corel Corporation'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). Corel Corporation'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 A.

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.

We assert that the controls within the system were effective throughout the period October 16, 2023, to October 15, 2024, to provide reasonable assurance that Corel Corporation's service commitments and system requirements were achieved based on the applicable trust services criteria.

Signed by:

Prashant Ketkar

10C7C5E2DD2B4F1...

Prashant Ketkar
Chief Product and Technology Officer
Corel Corporation

SECTION 2

Independent Service Auditor's Report

PRESCIENT ASSURANCE

Independent Service Auditor's Report

To: Corel Corporation

Scope

We have examined Corel Corporation's ("MindManager") accompanying assertion in Section I, titled "Management's Assertion" (the assertion) that the controls within Corel Corporation's MindManager system (the system) were effective throughout the period October 16, 2023, to October 15, 2024, to provide reasonable assurance that Corel Corporation'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).

Service Organization's Responsibilities

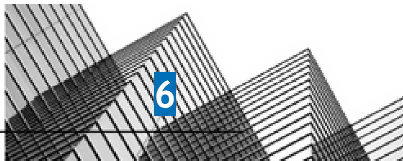
Corel Corporation is responsible for its service commitments and system requirements and for designing, implementing and operating effective controls within the system to provide reasonable assurance that Corel Corporation's service commitments and system requirements were achieved. In Section I, Corel Corporation has provided the accompanying assertion about the effectiveness of the controls within the system. When preparing its assertion, Corel Corporation is responsible for selecting, and identifying in its assertion, the applicable trust services 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 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 AICPA. 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 the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the controls are not effective to achieve Corel Corporation'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 Corel Corporation'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.

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 risks 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 the controls within Corel Corporation's MindManager system were effective throughout the period October 16, 2023, to October 15, 2024, to provide reasonable assurance that Corel Corporation's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

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

Prescient Assurance LLC

DocuSigned by:

Prescient Assurance

66274D51A66C4C8...

Prescient Assurance LLC

February 19, 2025

SECTION 3

Attachment A

Alludo

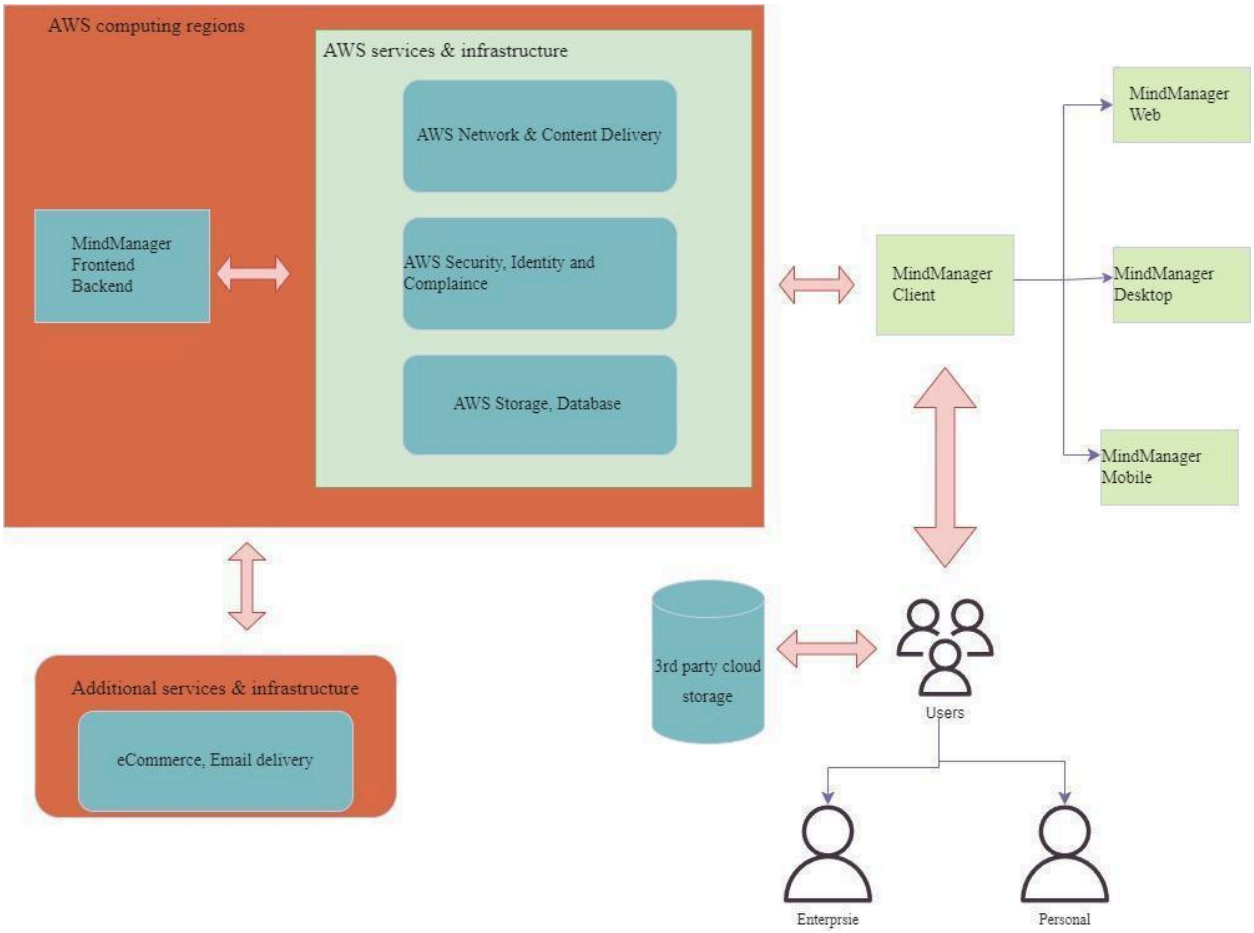
Company Overview and Types of Products and Services Provided

MindManager Cloud hereafter MindManager is part of Alludo's Productivity portfolio. The corporate headquarters is based in Ottawa Canada, while MindManager digital hosting is located in Europe and the Republic of Ireland. MindManager has a global customer base in over 200 countries and across 21 industries.

Alludo employs over 700 professionals, serving a diversified base of 90,000 million customers. Specific to MindManager customers, over 4.8M are supported through a fully digital environment located in Amazon Web Services (AWS). The production MindManager site is located in AWS Regional Edge Cache in Frankfurt Germany; the failover site is located in AWS Regional Edge Cache Dublin Ireland.

MindManager is a productivity tool enabling individuals, teams and enterprises to capture, process and share cross cutting information, transforming unstructured ideas and data into dynamic visual mind maps, diagrams.

MindManager is a multi-service, multi-tenant Software as a Service (SaaS) application deployed in a public cloud and managed through a shared responsibility model of protection. MindManager's information system consists of the following subsystems and boundaries.


AWS computing regions
AWS services & infrastructure
AWS Network & Content Delivery
AWS Security, Identity and Complaince
AWS Storage, Database
MindManager Frontend Backend
MindManager Client
MindManager Web
MindManager Desktop
MindManager Mobile
Additional services & infrastructure
eCommerce, Email delivery
3rd party cloud storage
Users
Enterprsie
Personal

User Profile Data is separated by a multi-tenant environment. Each tenant is identified by ID and all data is separated based on tenant ID.

For both data in transit and data at rest, a collection of digital enciphering techniques are implemented preventing data exfiltration and tampering, data exposure, and rendering protected data unrecoverable by unauthorized persons.

Shared Responsibility Model

As previously mentioned, MindManager is under a shared responsibility model for implementation and maintenance of security controls.

- European Union and European Parliament
- International Organization for Standardization
- Parliament of Canada
- U.S. Department of Commerce

Each of the policies defined in this document is applicable to the company’s digital and on-prem technology infrastructure and aligned to support global regulations and contractual obligations.

Additionally, the Company's credibility and future relationships are protected against brand tarnishment.

MindManager's information system is a virtualized pool of resources, functionalities, operating features, storage, databases, networking, software, analytics, and intelligence. The information system consists of subsystems and boundaries providing processing, maintenance, use, sharing, dissemination, or disposition of documents referred to as maps.

MindManager Account

A MindManager Account facilitates the validation of the services for each user and ensures that any data the user shares with the MindManager Cloud Services is owned, controlled and visible only to that user, unless the user selects to share that data with others.

Account creation requires the following information from the customer. They can be provided by a 3rd party Identity Provider or created by MindManager. The following user attributes are captured:

- name
- email address
- Password (for standard accounts only – SSO accounts do not have pw stored)
- agreement to Terms and Conditions and privacy policy
- 3rd party storage access tokens

Passwords are protected while in transit using the Secure Remote Password (SRP) Protocol between MindManager servers and AWS Cognito. Additionally, hashed passwords are stored in Amazon Web Services (AWS) RDS using the bcrypt $2b$ hash algorithm with 10 salt rounds and encrypted using AES-256 protecting against rainbow table and brute force attacks.

SRP is a class of strong authentication protocols that resists all well-known passive and active network attacks. It solves the problem of authenticating clients to servers securely. In cases where the user of the client software must memorize a small secret (like a password) and carries no other secret information. The server carries a verifier for each user, which allows it to authenticate the client but which, if compromised, would not allow the attacker to impersonate the client.

For customers using our Single Sign-on solution, passwords are not shared with MindManager, they are managed by their supported Identity Provider (IdP) such as:

- Microsoft Azure
- Google GSuite

A MindManager Account must be used to access MindManager Windows, MindManager Mac, MindManager for Microsoft Teams, MindManager Chromebook, MindManager Snap, MindManager Co-editing, MindManager Publishing, and/or Zapier. When a client ends their service agreement, they may request account deletion via the MindManager customer support team.

MindManager Encryption

Data is encrypted in transit between the end user client and MindManager servers through HTTPS and TLS. The TLS process uses asymmetric keys to secretly agree on a symmetric key that is then used by

both the client and MindManager server to exchange encrypted information for the duration of the data transfer sessions.

Data at rest is stored in Amazon Web Services (AWS) RDS (in a MySQL database) Data in RDS is encrypted using AES-256 Keys are securely managed by Amazon Web Services (AWS) Key Management Service which includes features like periodic rotation and storage of keys in separate locations. All external access is through TLS.

AWS Encryption mechanisms are industry standard and peer reviewed supporting FIPS 140-2 for data at rest and in transit; all are FIPS 140-2 validated

MindManager License Validation

MindManager's license administration portal user license validation ensures users are in compliance with the terms of their license agreement and/or contract. Users must connect to an online server when using MindManager products to validate that their MindManager account has a valid license to use the associated product.

MindManager License Administration Portal

The MindManager License Administration Portal allows the customers to administrate MindManager licenses including but not limited to viewing license keys, viewing number of used and available seats, viewing which users can use a license, and adding or removing users who can use a license. The following information can be viewed:

- email address
- license key(s)
- purchased product(s)
- Number of license(s) purchased
- Automatic provisioning settings
- SSO configuration
- Application settings
- License assignee email addresses

License key information itself is stored in Amazon RDS in a MySQL database. Data in RDS is encrypted using AES-256 Keys are securely managed through Amazon Web Services (AWS) Key Management Service which includes features like periodic rotation and storage of keys in separate locations. All external access is through TLS.

MindManager uses Twillio Sendgrid to handle transactional emails (EG license granted or revoked, seat coverage, etc) through their cloud-based service. Sendgrid provides domain authentication preventing sender masquerading along with TLS for all data in transit.

Sendgrid retains email message activity/metadata (such as opens and clicks) for 30 days. They store customer's aggregated sending stats and suppression lists (bounces, unsubscribes) and spam reports (which may contain content) indefinitely, and we store minimal random content samples for 61 days.

MindManager co-editing

Co-editing is a service that enables simultaneous editing of the same file by multiple users. Co-editing requires the user to provide the MindManager cloud with authorization to access at least one of their 3rd party storage providers. A high-level overview of the process follows:

1. The service temporarily stores files in the MindManager cloud during active co-editing sessions and saves changes from sessions back to the 3rd party storage provider of choice on the user's behalf.
2. Customer data from the co-editing session is deleted from the MindManager cloud after the file is saved back to the 3rd party provider.
3. In the event of an error saving on the user's behalf, the file is put in "recovery mode" where it is stored in the MindManager cloud for one week to allow the user to retrieve the file and any changes made during the co-editing session before it is permanently deleted.
4. Users can delete recovered files at any time before the one week has passed via the recovery UI.
5. Access to the MindManager Co-editing requires version 20.0 or greater for Windows and an active UPP plus MindManager Co-editing subscription, or an active MSA plus MindManager Co-editing subscription.

MindManager Go

MindManager Go is an installable mobile application for iOS and Android devices. The application allows users to open and view maps on their mobile device.

1. Users can authenticate in the application using their MindManager account which enables them to send data to the MindManager cloud via the MindManager Snap service integration within the mobile application.
2. Users can view and delete their content from the cloud via the Queue interface in the mobile app at any time.

Users can authorize the application to access their 3rd party storage providers to browse and open files from.

MindManager Publishing

Publishing is a service allowing users to easily share files with anyone with an Internet connection and a browser. A high-level overview of the process follows:

1. Publishing a file uploads it to the MindManager cloud where a unique URL is generated that can be used to access the file via an online viewing application.
2. Users can view and delete their previously published files at any time.

Trial users with a MindManager Account may try MindManager Publishing free of charge until their trial expires. Files published during the trial are automatically unpublished after 30 days.

MindManager Snap

MindManager Snap is a combination of products and services that send and receive information from the cloud; it is an optional service. It enables customers to quickly capture notes, links, and photos from the desktop, browser, or mobile device for later organization or use within MindManager software.

- Desktop Apps -Installable applications that allow users to easily send content like text, files, or links to be stored in our cloud for later retrieval and organization.
- Browser Extensions - Installable browser extensions that allow users to easily send content from web pages to be stored in our cloud for later retrieval and organization.
- Mobile Integration - Integrated into the MindManager Go mobile app for Android and iOS allowing users to easily send content from their mobile device like photos or text to be stored in our cloud for later retrieval and organization.
- Queue - Integrated into the MindManager editing applications, the Queue allows users to retrieve, organize, and move content stored in the cloud to a new location.
- About Customer Data - Users can view and delete their content from the cloud via the Queue interface at any time.

Access to MindManager Snap requires version 20.0 or greater for Windows AND Any of the following: MindManager purchased within the last 16 months, MindManager upgrade purchased within the last 16 months, active MSA subscription, active UPP subscription. Trial users with a MindManager Account may try MindManager Snap free of charge until their trial expires.

MindManager For Microsoft Teams

MindManager for Microsoft Teams is an integrated application that works on any platform* (Windows, Mac, Chromebook, iOS, Android) or web browser (Chrome, Firefox, Edge, Safari) supported by Microsoft Teams. The application allows users with the appropriate license to create, open, edit, co-edit, and save MindManager files in Teams.

MindManager for Microsoft Teams requires storage of files in Microsoft Teams with Microsoft SharePoint as the storage location and installation of the application in your Microsoft Teams instance. Files are not permanently stored on MindManager servers after editing. Files are deleted from MindManager servers after editing, changes are saved to Microsoft SharePoint during or after the session.

MindManager Co-editing requires storage of files in a supported 3rd party cloud storage service and authorization for the desktop application and web application to manage files on behalf of users who wish to co-edit using MindManager Co-editing. Supported services include Microsoft OneDrive, Google Drive, Microsoft SharePoint, Box, and Dropbox. MindManager is not responsible for the security or privacy of files stored in 3rd party cloud storage services. It is the responsibility of the customer to secure their Teams and SharePoint instances against intrusions.

MindManager for Microsoft Teams is limited to a maximum of 30 concurrent editors per file. Maximum concurrent users can vary depending on network and computing capabilities.

Data in Process (while an editing or co-editing session is in progress) is stored in Amazon Web Services (AWS) Redis, Lambda, S3, and RDS. Whereas data in Redis, Lambda, S3, and RDS is encrypted using AES-256.

Keys are securely managed by Amazon Web Services (AWS) Key Management Service which includes features like periodic rotation and storage of keys in separate locations. All external access is through TLS.

Data at rest stored in RDS is encrypted using AES-256 and bcrypt $2b$ hash algorithm with 10 salt rounds where applicable. Keys are securely managed by Amazon Web Services (AWS) Key Management Service which includes features like periodic rotation and storage of keys in separate locations, all external access is through TLS.

File data is sometimes stored at rest in Amazon Web Services (AWS) S3. File data is stored at rest for the MindManager for Microsoft Teams app when there is a problem saving the MindManager file with changes from the editing session back to the original cloud storage location, all data stored at rest for this service is automatically deleted after 7 days, after the file is successfully saved back to the provider, or when the user opts to delete it, whichever occurs first Data in S3 is encrypted using AES-256 Keys are securely managed by Amazon Web Services (AWS) Key Management Service which includes features like periodic rotation and storage of keys in separate locations. All external access is through TLS.

Zapier integration

Zapier allows users to send and receive information to or from thousands of 3rd party services by creating rules in the Zapier interface.
Utilization of the service requires a Zapier® account, authorization for Zapier to access the users MindManager data, and authorization for the MindManager to access the users Zapier® data. A high-level overview of the process follows:

- Data sent to MindManager from Zapier® is stored in the MindManager cloud until the user receives the data in the MindManager application, after which time it is permanently deleted from the cloud.
- Data sent to Zapier® from MindManager is managed by Zapier® and deletion of that data is handled via the Zapier® website/application.

Access to the MindManager Zapier® Service requires version 18.0 or greater for Windows, and a Zapier® account.

The 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 ProLink has established for the services.

Security commitments to user entities are documented and communicated in 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 Components of the System Used to Provide the Services

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.

Information facilitation is achieved across the various components comprising the information are Sub-system(s) and Boundaries.

Procedures

Policies, procedures, and standards have been developed outlining authorities and responsibilities for the system and its users. Policies related to IT security are reviewed and approved by management annually.

Boundary

To us, a boundary is the set of information resources allocated to an information system defines the boundary for that system. Organizations have significant flexibility in determining what constitutes an information system and its associated boundary. Boundary protection controls are defined by NIST 800-53r5.

The current environment is secured through a blend of available digital and transitional logical and virtual components protecting information from disclosure, theft and exfiltration. Transitional boundaries are physical, logical and virtual mechanisms when interconnected, providing access traversal throughout an information system.

The current mechanisms providing boundary control are:

1. Security Groups – where rules enable traffic filtering based on protocols and port numbers
2. Port filtering - where the destination port and IP are explicit
3. Environment segregation based on a three-legged design – where subnets are deployed creating logical segregation of sub-systems
4. Traffic flow controls – where destination and protocol of ingress and egress is explicit
5. Logging and Monitoring – where events indicating Indicators of compromise (IoC) are aggregated in our SIEM for notification and response

The Applicable Trust Services Criteria and the Related Controls Designed to Provide Reasonable Assurance that the Service Organization's Service Commitments and System Requirements were Achieved

Management's Philosophy and Operating Style

MindManager's control environment reflects the philosophy of senior management concerning the importance of security of customer data and information. MindManager Oversight Board exercises oversight of the development and performance of internal control through bi-annual meetings. MindManager Executive Management meets on a weekly basis to discuss product, operations, and information technology.

The objectives of internal control as it relates to the MindManager System are to provide reasonable, but not absolute, assurance that controls are suitably designed and operating effectively to meet the relevant controls, that assets are protected from unauthorized use or disposition, and that transactions are executed in accordance with management's authorization and client instructions. Management has established and maintains controls designed to monitor compliance with established policies and procedures. The remainder of this subsection discusses the tone at the top as set by management, the integrity, ethical values, and competence of MindManager employees, the policies and procedures, the risk management process and monitoring, and the roles of significant control groups. The internal control structure is established and refreshed based on MindManager's assessment of risk facing the organization. MindManager's internal control components include controls that may have a pervasive effect on the organization, or may affect specific processes or applications, or both. Some of the components of internal control include controls that have more of an effect at the entity level, while other components include controls that are primarily related to specific processes or applications.

Organizational Structure and Assignment of Authority and Responsibility

MindManager's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

MindManager's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

Human Resource Policies and Practices

MindManager's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. MindManager's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgement forms for the code of conduct and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

Change Management

Change management and systems development lifecycle (SDLC) policies are formally documented, communicated and available to employees. The policy is reviewed and updated at least annually. Emergency changes follow the change management process and are documented within JIRA. All product changes are required to have an associated JIRA ticket. QA performs testing and approval at multiple levels before a change is implemented. All releases are reviewed and approved by the Operations Manager and Product Owner before implementation. Developers cannot push a change to production. Development and production environments are logically separated.

Risk assessment process

The Board of Directors meet at least quarterly to discuss product, operations, and information technology.

At least annually the information systems undergo risk assessments based on various frameworks supporting identification of improvement and prioritization resulting in a multi-year roadmap that is a blend of strategic and tactical projects.

Information and communication systems

Information and communication are an integral component of MindManager's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations.

MindManager uses several information and communication channels internally to share information with management, employees, contractors, and customers. MindManager uses chat systems and email as the primary internal and external communications channels.

Structured data is communicated internally via SaaS applications and project management tools. Finally, MindManager uses in-person and video "all hands" meetings to communicate company priorities and goals from management to all employees.

Security Management

Monitoring software is used to identify and evaluate ongoing performance, security threats, utilization levels, and to flag unusual activity. The software notifies IT personnel when predefined events are detected, and a corresponding ticket is created. Paging software is integrated with monitoring tools to notify appropriate personnel when predefined security events are identified. Additionally, As part of our commitment to robust security practices, our company has engaged a Managed Detection and Response (MDR) service. Which is a cybersecurity service that provides 24/7 monitoring, detection, and response to cyber threats. The MDR service employs advanced threat detection technologies and expert analysts to identify and respond to potential security incidents in real-time. By leveraging this proactive approach, we enhance our ability to detect, investigate, and mitigate cyber threats promptly, thereby strengthening our overall security posture and ensuring the protection of our systems and data.

As part of our comprehensive security strategy, our company annually engages third-party security firms to conduct two distinct penetration tests. The first is a broad assessment targeting our entire corporate infrastructure, while the second is a focused evaluation specifically for the MindManager application. These thorough assessments help identify potential vulnerabilities, validate our security controls, and ensure the integrity of both our overall systems and the MindManager application in particular. This dual approach demonstrates our commitment to maintaining robust security measures across all aspects of our operations.

Monitoring controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. MindManager's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-going monitoring

MindManager's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in MindManager's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of MindManager's personnel.

Complementary Subservice Organization Controls (CSOCs)

MindManager's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to MindManager's services to be solely achieved by MindManager control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of MindManager.

The following subservice organization controls have been implemented by AWS and included in this report to provide additional assurance that the trust services criteria are met.

AWS

Category	Criteria	Control
Security	CC 6.4	Data center server floors, network rooms and security systems are physically isolated from public spaces and/or delivery areas.
Security	CC 6.4	Access to sensitive data center zones requires approval from authorized personnel and is controlled via badge access readers, biometric identification mechanism, and/or physical locks.
Security	CC 6.4	Data center perimeters are defined and secured via physical barriers.
Security	CC 6.4	Access lists to high security areas in data centers are reviewed on a defined basis and inappropriate access is removed in a timely manner.
Security	CC 6.4	Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of the visit.
Security	CC 6.4	Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.
Security	CC 6.4	Data centers are continuously staffed and monitored by security personnel using real time video surveillance and/or alerts generated by security systems.

Any Specific Criterion of the Applicable Trust Services Criteria that is Not Relevant to the System and the Reasons it is Not Relevant

All Common Criteria/Security, Security criteria were applicable to the MindManager's system.