Service Organization Control 3 (SOC 3)

For the Period April 1, 2023 to March 31, 2024

Report of monday.com Work Operating System

Relevant to Security, Availability, Confidentiality and Privacy

Kost Forer Gabbay & Kasierer
144 Menachem Begin St.
Tel-Aviv 6492102, Israel

Tel: +972-3-6232525
Fax: +972-3-5622555
ey.com

Independent Service Auditor's Report

To the Management of monday.com:

Scope:

We have examined management's assertion, contained within the accompanying Management Assertion of monday.com Ltd. (Assertion), that monday.com Ltd.'s controls over the monday.com Work Operating System (System) were effective throughout the period April 1, 2023, to March 31, 2024, to provide reasonable assurance that monday.com Ltd.'s service commitments and system requirements were achieved based on the trust services criteria relevant security, availability, confidentiality and privacy] (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.

monday.com Ltd. uses Amazon Web Services (subservice organization) as an infrastructure management service. The description of the boundaries of the system presented in Appendix A indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with related controls at monday.com Ltd., to provide reasonable assurance that monday.com Ltd.'s service commitments and system requirements are achieved based on the applicable trust service criteria. The description of the boundaries of the system presents the types of controls that the service organization assumes have been implemented, suitably designed, and operating effectively at Amazon Web Services. Our procedures did not extend to the services provided by Amazon Web Services and we have not evaluated whether the controls management assumes have been implemented at Amazon Web Services have been implemented or whether such controls were suitably designed and operating effectively throughout the period April 1, 2023 to March 31, 2024.

Management's responsibilities

monday.com Ltd.'s management is responsible for its service commitments and system requirements, and for designing, implementing, operating, and monitoring effective controls within the system to provide reasonable assurance that monday.com Ltd.'s service commitments and system requirements were achieved. monday.com Ltd. management is also responsible for providing the accompanying assertion about the effectiveness of controls within the System, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the System and describing the boundaries of the System.
- Identifying the service commitments and system requirements and the risks that would threaten the achievement of the service commitments and service requirements that are the objectives of the System.

Our responsibilities

Our responsibility is to express an opinion on the Assertion, based on our examination. 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. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of monday.com Ltd.'s relevant: security, availability, confidentiality, and privacy policies, processes, and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we consider necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating monday.com Ltd.'s cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

We are required to be independent of monday.com Ltd. and to meet our other ethical responsibilities, as applicable for examination engagements set forth in the Preface: Applicable to All Members and Part 1 – Members in Public Practice of the Code of Professional Conduct established by the AICPA.

Inherent limitations:
Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve monday.com Ltd.'s service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the System or controls, or the failure to make needed changes to the System or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Opinion:
In our opinion, monday.com Ltd.'s controls over the System were effective throughout the period April 1, 2023, to March 31, 2024, to provide reasonable assurance that its service commitments and system requirements were achieved based on the applicable trust services criteria.

Restricted use
This report is intended solely for the information and use of monday.com Ltd. and is not intended to be, and should not be, used by anyone other than these specified parties.

Very truly yours,

Kost Forrer Gabbay and Kasierer

Kost Forrer Gabbay & Kasierer
A member firm of Ernst & Young Global
May 8, 2024
Tel Aviv, Israel

Management Assertion on the controls over monday.com Work Operating System, based on the AICPA Trust Services Principles and Criteria for Security, Availability, Confidentiality and Privacy

We, as management of, monday.com Ltd. ("monday.com" or " the Company") are responsible for:

- Identifying the monday.com Work Operating System (system) and describing the boundaries of the system, as presented in Appendix A.
- Identifying our service commitments and system requirements.
- Identifying the risks that would threaten the achievement of our service commitments and service requirements that are the objectives of our system, which is presented in Appendix A.
- Identifying, designing, implementing, operating, and monitoring effective controls over the monday.com Work Operating System (system), to mitigate risks that threaten the achievement of the service commitments and system requirements.
- Selecting the trust services categories and associated criteria that are the basis of our assertion.

monday.com Ltd. uses Amazon Web Services to identify the function or service provided by the subservice organization. The description of the boundaries of the system presented in Appendix A indicates that complementary controls at Amazon Web Services that are suitably designed and operating effectively are necessary, along with controls at monday.com Ltd. to achieve the service commitments and system requirements. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of monday.com Ltd.'s controls. It does not disclose the actual controls at Amazon Web Services.

We confirm to the best of our knowledge and belief that the controls over the System were effective throughout the period April 1, 2023 to March 31, 2024, to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality and privacy (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.

Yours sincerely,

Signature Eran Zinman

Title DocuSigned by: 9734413E9EF64B8...

Appendix A - Description of the monday.com Work Operating System

Company Overview and Background

The company was founded in February 2012 and the product was launched as an independent startup in 2014. The company also became public in June 2021. The monday.com Work OS is a low code-no code platform that democratizes the power of software so organizations can easily build work management tools and software applications to fit their every need. The platform intuitively connects people to processes and systems, empowering teams to excel in every aspect of their work while creating an environment of transparency in business. monday.com has offices in Tel Aviv, New York, Miami, Chicago, Denver, London, Warsaw, Sydney, Melbourne, São Paulo, and Tokyo. Fully customizable to suit any business vertical, the platform is currently used by over 225,000 customers across more than 200 industries and in over 200 countries and territories.

Organizational structure

monday.com's organizational structure provides the overall framework for planning, directing, and controlling operations for the monday.com Work Operating System. It utilizes an approach whereby personnel and business functions are segregated according to job responsibilities. This approach allows the Company to clearly define responsibilities, lines of reporting, and communications and allows employees to focus on the specific business issues impacting their clients.

Chief Executive Officer (CEO) - The CEOs are responsible for all company's operations and activities, and report on a quarterly basis to the Board. The CEOs conduct weekly meetings with the C-Suite level team and review all company activities including security and compliance efforts.

Chief Information Security Officer (CISO) - monday.com invests significant resources to help ensure the security of their services and data. The Chief Information Security Officer (CISO) is responsible for defining and building the company's security roadmap, prioritizing efforts based on the company's key assets, and implementing and enforcing security processes and controls. The CISO is involved in processes to monitor that the security procedures are maintained throughout monday.com operations. Ongoing risk management processes are conducted, security controls are defined (operational, physical, and logical) and third-party vulnerability penetration tests are managed, among other activities, ensuring that production risks, exposures, and vulnerabilities are identified, controlled, and managed.

Data Privacy Officer (DPO) - monday.com invests significant resources to help ensure the security of its services and data. The Data Privacy Officer (DPO) is an outsourced worker from an external privacy consulting company, which is involved in processes to monitor that the privacy procedures are maintained throughout monday.com's operations. Ongoing risk management processes and Privacy Impact Analysis are conducted, Privacy by Design is implemented throughout the development life cycle, and privacy controls are defined (operational, physical, and logical). The DPO is the point of contact for customers with privacy-related inquiries or complaints, as required by the GDPR.

Customer Experience - monday.com provides technical support 24 hours a day, 7 days a week, 365 days a year. The Customer Experience process consists of internal and external automated monitoring services and is designed to enable internally identified issues related to clients and requests raised by clients to be handled and resolved. monday.com client support procedures are designed to handle and resolve issues and requests timely and efficiently. These include issues that are internally identified or submitted by clients. Each issue that is identified by monday.com or reported by monday.com customers is assigned a severity level and is tracked according to the SLA.

Research and Development (R&D) - The Research and Development (R&D) department is responsible for designing and developing new features and capabilities of the monday.com Work Operating System, according to functional requirements and specifications driven by client and market needs as determined by the Management Team, and in

accordance with monday.com's internal security and privacy policies and guidelines.

Chief Revenue Officer (CRO) - The CRO department's duties and responsibilities are:

- Service existing accounts, obtain orders, and establish new accounts.
- Adjust the content of sales presentations by studying the type of sales outlet.
- Focus sales efforts by studying the existing and potential needs of clients.
- Keep management informed by submitting activity and results reports, such as daily call reports, weekly work plans, and monthly and annual territory analyses.
- Recommend changes in products, services, and policies by evaluating results and competitive developments.
- Resolve customer complaints by investigating problems, developing solutions, preparing reports, and making recommendations to management.

People - System controls are only as strong as the people that implement them. monday.com commits to employ competent individuals who possess the skills required to successfully implement the company's objectives. Products and services are created and delivered by the company's developers, product and design managers, among others, and customer experience managers. Employees are hired in line with hiring policies and procedures.

Components of the system providing the defined services

monday.com's Policies and Communication

monday.com's management requires formal written policies for significant functions and processes. These policies are shared with all monday.com employees and are reviewed, and approved annually by the management. In addition, roles and responsibilities for developing and maintaining these policies are assigned.

Significant components of these policies include, among others:

- Organizational structure.
- Responsibility for information assets.
- Data classification.
- Access Control.
- Security & Data incident response.
- Change management.
- Physical security.

A description of the monday.com Work Operating System and its boundaries is documented and communicated to monday.com employees and customers within the internal portal and the monday.com application. monday.com has implemented multiple communication channels to monitor that processes function as they were designed, and potential issues are identified and resolved in a timely manner. Various operations and synchronization meetings are generally conducted on a periodical basis in accordance with the operational needs. monday.com managers are responsible for communicating relevant corporate information and job-related data to their direct employees.

Availability, confidentiality, and security-related obligations are communicated to monday.com's employees through confidentiality and non-disclosure agreements while client obligations are communicated within their contracts. In addition, an incident management application is available to monday.com employees to report security, availability, and confidentiality incidents. Customer issues are reported within a dedicated CRM application.

Security and Logical Access

Overview

monday.com's production environment is hosted in Amazon Web Services data centers across multiple availability zones. The production environment includes multiple AWS cloud components such as EC2 instances, Elastic Load Balancers, Lambda functions, SQS, SNS resources, and more. The company also uses multiple database technologies such as relational database systems (e.g. MySQL, PostgreSQL), NoSQL (e.g. DynamoDB and MongoDB), and in-memory databases. Databases are redundant within the production environment.

monday.com production network encompasses numerous components, including segmented internal networks, security and monitoring tools, and services responsible for redundancy and scaling. The production network is built on several tiers, where each type of server has its own segment and access rules. The AWS infrastructure consists of synchronization components that can be scaled up when needed. The network is monitored using a network intrusion detection system. Administrative access to the AWS management interface is restricted to authorized personnel.

Logical Access

monday.com has established an information security policy designed to protect information at a level commensurate with its value (refer to the policy section above). The policy dictates security controls for media where information is stored, the systems that process it, as well as infrastructure components that facilitate its transmission. New users who are granted access to the production environment and database are approved by monday.com's DevOps.

Production environment – AWS

As mentioned above, monday.com's production environment is hosted in Amazon Web Services data centers across multiple availability zones.

User Permissions management

monday.com manages and delivers its services using AWS. Information security controls and procedures are implemented throughout these systems to help prevent unauthorized access to data. Access to system resources is protected through a combination of firewalls, native operating system security, database management system security, application controls, and intrusion detection monitoring software. monday.com employees are provided with unique, personal user accounts that enable them to access the corporate cloud account. Users are identified through the use of a user ID/ password combination using AWS, the application, and the database. Employees are provided with the minimal access rights required to carry out their duties. Access to the production environment, where information resources that are not deemed to be public reside, including the domain, databases, and other production related environments, is granted upon approval by the IT or DevOps Team. In addition, access to the database is restricted to authorized personnel only.

Usernames and passwords are used to authenticate personnel who need to access a system or a resource. Where applicable, strong password configuration settings are enforced through a directory service, including: (1) forced password change at defined intervals, (2) a minimum password length, (3) a limit on the number of attempts to enter a password before the user ID is suspended, and (4) password complexity. Due to system limitations, some configuration parameters may not be available on certain systems.

Recertification of Access Permissions

monday.com has implemented an access recertification process to help monitor that only authorized personnel have access to the systems, environments, and databases. Permissions with the different environments are reviewed and approved by the monday.com infrastructure team on a quarterly basis.

Access Revocation

User accounts are disabled or deleted on the production, application, and database and the Company's assets are returned timely upon notification of job termination. Termination notifications indicating the employee's expected last day are sent to the relevant function: Management, HR, Finance, and IT. Terminated employees complete a termination clearance process on their last day at monday.com. This process includes the revocation of access permissions to the systems and premises, as well as the return of the Company property, data, and equipment.

Physical Access

monday.com recognizes the significance of physical security controls as a key component in its overall security program. Physical access methods, procedures, and controls have been implemented to help prevent unauthorized access to data, assets, and restricted areas. Physical access to monday.com's office is restricted to authorized personnel using fingerprint identification. Visitors to the monday.com office are accompanied while on premises.

Remote Access

monday.com networks are protected using firewalls, which are configured and administered by the IT Manager, and security tools provided by the AWS service providers. monday.com employees are granted remote access to the production environment based on the need-to-know principle. In addition, remote site-to-site access to the production network is accomplished through a secured connection and is restricted to company personnel only. monday.com's information security policies require employees who are granted remote access permission to protect their workstations from unauthorized users, and all employees' workstations are secured using antivirus software. Also, customers' environments are segregated at the application and database level using unique IDs that are the result of a combination of several parameters. These are set when the customer registers to the application.

Vulnerability and penetration testing

monday.com's security program includes testing for security vulnerabilities by an independent security assessment service provider. A penetration test is performed on an annual basis. High issues are investigated and taken care of as part of the SDLC process or by any necessary means. In addition, monday.com has a managed bug bounty program, through which security researchers from around the world are allowed to privately and responsibly disclose security vulnerabilities they have found, in exchange for a monetary reward. The penetration testing includes, among others, procedures to prevent customers, groups of individuals, or other entities from accessing confidential information other than their own. Input fields from the monday.com application are automatically sanitized in order to prevent code injection. In addition, automated vulnerability tests are performed on the production environment on a quarterly basis in order to detect potential security breaches.

Security Awareness and Training

To help ensure that monday.com employees are aligned with the security practices and are aware of their duties, monday.com has implemented an internal security awareness program, including conducting a quiz to measure the effectiveness of this program. monday.com's employees are going through security awareness training on at least an annual basis. Regarding regulatory requirements, such as HIPAA Security Requirements and GDPR, the company has established a dedicated program communicated to all departments to ensure they understand the regulations and their requirements.

Software Development Lifecycle ("SDLC") and Change Management

Software development at monday.com is performed in a controlled manner, to help ensure applications are properly designed, tested, approved, and aligned to the monday.com business objectives. Personnel responsible for the design, development, implementation, and operation of systems affecting Security, Availability, and Confidentiality issues have the qualifications and resources to fulfill their responsibilities. The R&D team conducts regular sessions and training to ensure the teams are up to date with the latest technologies and techniques, as well as the latest threats and methods to mitigate them. Changes are documented and prioritized using tasks within the change management application. The changes are connected to the source control in order to link the request to the actual code change. The permission to merge tested versions into Master branches is restricted to authorized personnel. Access to the source control application is restricted to authorized personnel.

The code is verified manually in the local and staging environment. During the testing stage the code goes through 8 specific phases and includes tests:

1. Static code analysis for bugs and vulnerabilities.
2. Secrets or passwords that are hard-coded into the code.
3. Dangerous code usages defined by monday.com
4. Unit test
5. End-to-end test
6. Integration test
7. Automatic detection of potential security vulnerabilities in its dependencies.
8. Code coverage monitoring which reports current levels and recent code coverage changes.

A Continuous Integration (CI) tool is used to monitor testing phases. Pull requests are performed in order to deploy code changes. The pull requests include, among others: (1) Mandatory code review, (2) An automated security code review, and (3) Testing. Code changes are reviewed along with the pull request performed by the developer. The code review is documented within the pull request itself. Code review is mandatory in order to continue in the SDLC process and deploy a version to the production environment. monday.com performs end to end tests that are running as part of the CI/CD tool. Only after all preliminary checks have passed, the dedicated developers will deploy the code to the production environment.

Change Initiation

New feature developments are initiated by the Product Team while technical improvements, bug fixes, and security requirements are initiated by clients and reviewed by the R&D Team. Changes to the database environment needed to support application changes are performed according to defined procedures, reviewed by the database administrator, and tracked in a dedicated change management application that includes a history of changes and approvals. In addition, significant changes performed to the application are communicated to the relevant monday.com customers within the monday.com application. Changes performed to the production environment are followed by a notification to key monday.com personnel via an internal communication tool.

Monitoring

Changes that may affect system security, availability, or confidentiality are defined and communicated through the change management application. monday.com implements segregation of duties throughout its change management process. The production environment is restricted to authorized personnel on a need-to-know basis and least privileges, enabling monday.com to minimize the possibility of unauthorized changes.

Infrastructure Change Management Overview

monday.com regularly makes changes within its production environment in response to change requests. These changes include routine maintenance activities, virtual machine and software updates, and other infrastructure-related changes. Change management procedures have been implemented by the Infrastructure Team Leader to help manage and maintain the production environment in an orderly and controlled manner. The change management procedure supports the business objectives of monday.com's clients and ensures the availability, confidentiality, security, and privacy of monday.com's services and data. monday.com uses its internal portal to manage key tasks, such as the identification, prioritization, assignment, resolution, and notification required by enterprise-critical functions. monday.com's change management processes incorporate the following key components:

- Approval of changes prior to implementation;
- Documentation of change requests, workflow, and history in the ticketing system;
- Execution of major changes within a defined maintenance window in order to minimize potential risks to services and clients.

Support and Operations

monday.com's customer support procedures are designed to handle and resolve issues and requests in a timely manner. This includes issues that are internally identified or issues submitted by clients. All customers are provided with 24/7/365 support via support mail, chatbot, live chats, callbacks, and customer support portal. Support is handled by monday.com according to its internal Service Level Agreement procedure.

A customer experience (CX) department is available at monday.com to provide support to its customers. Issues raised to the CX department are documented within the CRM tools. Customer issues are addressed based on the internal SLA policy and procedures.

Additionally, monday.com opens a ticket when an issue raised by a client requires development Support meetings with the management are performed on a weekly basis to report major open issues to the management.

Escalation Process

Ticket escalation is done automatically through the system. monday.com's objective as it relates to escalation is to resolve issues during the first contact. If the first contact cannot resolve the issue, the issue is escalated to the next level of technical support. The escalation process is defined and documented in a matrix managed by Customer Experience. A dedicated internal system is used to track and manage bugs. Decisions regarding the bug status are updated during bi-weekly iteration meetings with the R&D team leaders. Service interruptions are communicated to monday.com's customers according to the internal escalation procedure through the status page.

Emergency Procedures

An emergency change is a change deemed critical enough that it is implemented outside of the regular maintenance window and does not follow the routine approval process. In the case of an emergency change, authorized personnel make the change to maintain the level of service in the production environment. Emergency changes are documented, reviewed, and approved in an escalated process. Changes performed to the production environment are followed by a notification to key monday.com personnel via an internal communication tool.

Availability procedures

Database backup and restoration

monday.com utilizes AWS backup services for the management and performance of backup tasks of various types of service-related data retained within the production environment, to enable the availability and redundancy of data. Databases are redundant within the production environment. The monday.com application database is backed up according to the backup policy. The monday.com databases are replicated to the cloud backup application.

Disaster Recovery Plan (DRP)

monday.com has developed a Disaster Recovery Plan to enable the company to continue to provide critical services in case of a disaster. The Disaster Recovery Plan is tested at least twice a year to assess its effectiveness and to keep the teams aligned with their responsibilities in case of a service interruption.
monday.com maintains a redundant infrastructure located at multiple locations within AWS environments. Those servers have been designed to provide clients with high availability services.

Confidentiality Procedures

Customer confidentiality is a key factor for monday.com. As such, monday.com has implemented security measures to ensure the confidentiality of its customers' sensitive personal information. The security measures aim to prevent unauthorized access, disclosure, alteration, or destruction of sensitive personal information. A confidentiality agreement is disclaimed as it relates to contracts with infrastructure third party providers, in accordance with monday.com security policy. monday.com maintains policies regarding the return, transfer, and disposal of user data and makes these policies available to customers. Upon customer request, at the conclusion of a contractual agreement, monday.com will dispose of customer confidential information.

Privacy Procedures

Management

Responsibility and accountability are assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating monday.com's privacy policies. The names of such a person or group and their responsibilities are defined. To help ensure that monday.com employees are aligned with security practices and are aware of their duties with regards to data privacy, monday.com has implemented security and privacy awareness training detailing the secure handling of company confidential information, including customer data. The mandatory training is conducted for new and existing employees.

Notice

monday.com provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy. The monday.com privacy policy is available on its website and fully discloses the type of information the company may collect from the monday.com application and website, as well as how monday.com may use this information. The monday.com privacy policy is reviewed and updated by management on at least an annual basis.

As a responsible business, monday.com recognizes at senior levels the need to comply with the GDPR and ensure that effective measures are in place to protect the personal data of its customers, employees, and other stakeholders.

As part of meeting its legal obligations, an information security policy is available in both paper and electronic forms and is communicated within the organization and to all relevant stakeholders.
Commitment to the delivery of information security extends to senior levels of the organization and is demonstrated through the information security policy and the provision of appropriate resources, in order to establish and develop effective information security controls.

Top management also ensures that a systematic review of the performance of the program is conducted on a regular basis to ensure that information security objectives are being met and relevant issues are identified through the audit program and management processes.

A risk management approach and process are used which are in alignment with the requirements and recommendations of the GDPR and relevant international standards such as ISO/IEC 27001:2013.

Risk management takes place at several levels within the organization, including:

1. Assessment of risks to the achievement of information security objectives
2. Regular information security risk assessments within specific operational areas
3. Assessment of risk as part of the business change management process
4. At the project level as part of the management of significant change

****