Miro

System and Organization Controls Report (SOC 3)

Independent Report of the Controls to meet the criteria for the Security, Availability, and Confidentiality categories for the period of January 1, 2021 through December 31, 2021.

KirkpatrickPrice

4235 Hillsboro Pike
Suite 300
Nashville, TN 37215

TABLE OF CONTENTS

ASSERTION OF MIRO MANAGEMENT

ASSERTION OF MIRO MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Miro's online collaborative whiteboard platform system (system) throughout the period January 1, 2021, to December 31, 2021, to provide reasonable assurance that Miro's service commitments and system requirements relevant to Security, Availability, and Confidentiality were achieved. Our description of the boundaries of the system is presented in section 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 January 1, 2021, to December 31, 2021, to provide reasonable assurance that Miro's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (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*). Miro'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 section B.

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 January 1, 2021, to December 31, 2021, to provide reasonable assurance that Miro's service commitments and system requirements were achieved based on the applicable trust services criteria.

INDEPENDENT SERVICE AUDITOR'S REPORT

Andrey Khusid
CEO
Miro
201 Spear Street, Suite 1100
San Francisco, CA 94105

Scope

We have examined Miro's accompanying assertion titled "Assertion of Miro Management" (assertion) that the controls within Miro's online collaborative whiteboard platform system (system) were effective throughout the period January 1, 2021, to December 31, 2021, to provide reasonable assurance that Miro's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (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

Miro is responsible for its service commitment and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Miro's service commitments and system requirements were achieved. Miro has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Miro 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 American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

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

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

Inherent Limitations

There are inherent limitations in 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.

Opinion

In our opinion, management's assertion that the controls within Miro's online collaborative whiteboard platform system were effective throughout the period January 1, 2021, to December 31, 2021, to provide reasonable assurance that Miro's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Joseph Kirkpatrick
CPA, CISSP, CGEIT, CISA, CRISC, QSA
4235 Hillsboro Pike, Suite 300
Nashville, TN 37215

February 11, 2022

MIRO'S DESCRIPTION OF ITS ONLINE COLLABORATIVE WHITEBOARD PLATFORM SYSTEM

SECTION A:
MIRO'S DESCRIPTION OF THE BOUNDARIES OF ITS ONLINE COLLABORATIVE WHITEBOARD PLATFORM SYSTEM

Services Provided

Miro offers an online collaborative whiteboard platform that enables remote team users such as product managers, designers, agile coaches, marketers, and other professionals to add pictures, mock-ups, drawings, videos, sticky notes, office documents, and Google Drive files on an endless canvas and collaborate, visualize, and share their ideas, daily regardless of their location.

Miro's basic tools include the following:

- Whiteboarding tools: sticky notes, freehand drawing, shapes, links, texts, presentation mode
- Collaboration tools: real-time collaborative editing, comments, text chat, voice and video chat, screen sharing, daily notifications
- Sharing and export tools: invite other people via email, export boards as images and pdf files, save to Google Drive, post to Facebook, embed into blogs and websites
- Visual libraries: prototyping, tables and charts, business canvases, templates for design thinking, project management, brainstorming and creative sessions

This system can be integrated with Atlassian Jira and Confluence, Sketch, Slack, Trello, Box, Google Drive, and more.

Internal Sales personnel utilize marketing engines and software resellers to generate sales leads for the Enterprise services. Sales processes are tracked through Salesforce. Once sells are won, agreements between the customers and Miro are signed, notifications are sent from the Salesforce system to the Onboarding team and the Support team to provision the account within Miro's systems.

The Onboarding team will create an account in the Gainsight CSM tool which is utilized to manage the implementation. The Support team creates the client profile and team account and enters the number of licenses purchased in the Miro. A client queues and workflows are created in the Zendesk system. If needed, data migration, the process of bringing existing independent accounts under the corporate account, is performed.

Smaller companies or companies with smaller needs can obtain Free, Team, and/or Business services directly from the website after agreeing to Miro's Terms of Service and creating a user account.

Once the account has been created, the client is responsible for adding and/or removing access to the accounts and/or boards.

Offboarding of Enterprise clients starts once a client has provided notification that the relationship is terminating. A departure date is set and, on that date, the queues in the Zendesk ticketing system

and the accounts in the Miro system are removed/disabled. Client data is either obtained directly from the client or through the assistance of Miro personnel up to 180 days after closing the account. Data is not recoverable after 180 days.

Smaller companies or companies with smaller needs can terminate at the end of their current month and can stop paying. Client data can be downloaded and/or deleted directly from the account.

Infrastructure

The company documents its network design for purposes of showing how the office location communicates and shares resources from the Amazon Web Services (AWS) Cloud environment and how the office location is protected and segmented using Web Application Firewalls (WAFs). To outline the topology of its network, the organization maintains network diagrams to illustrate its internal infrastructure. The diagrams are reviewed and updated at least annually.

All critical assets are identified in the diagrams as well as a systems inventory. The system inventory is maintained with automated tools. For the production and test environments, ansible scripts and AWS CLI are used. For the office's inventory, Jamf is used. The DevOps team is responsible for the production and test environments. Internal tools, as well as the IT infrastructure team, are responsible for the office's inventory. Inventories are updated once a change had been applied.

Software

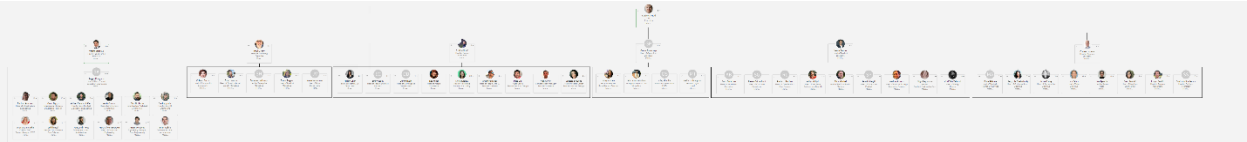
The software inventory list is reviewed annually. Business-critical software is listed in the asset inventory tab of the corporate risk assessment with indication of its function. Licensing information is maintained separately by IT management with the access matrix and reporting is performed using Black Duck Licensing review software.

The trust team, team leads, and asset owners are involved to validate assets and related information (e.g., description, business risk level). Licensing information is maintained by IT management. The information is updated ad-hoc with involvement of the team leads and legal team. Licensing information of libraries in use inside the app is supervised by the security and legal teams. Black Duck Software Composition Analysis (SCA) scans the application source code and provides information about licenses in use.

People

The organization maintains a hierarchical structure with functional business units. The organization's hierarchy includes Executive and Middle Management with a functional structure of departments and teams. The organization maintains a full organizational chart that illustrates division, department, location, and direct reports for all employees. The Human Resources (HR) team is responsible for maintaining the Miro organizational chart.

The board of directors meets quarterly and is involved in planning, monitoring, and managing financial resources. The board of directors selects officers and executives for overseeing operation and development. The chart included below is generated from the HR system.



Data

Miro has an approved Data Protection Policy that describes all types of data involved into the entity's operation. Miro's online whiteboarding solution generally processes and stores two types of data: profile data (name, second name, and email of the user needed to distinguish the accounts) and information provided by users without inspection (uploaded to the app). All such information is maintained as confidential and private to the owner user. This confidential and private information is available only to the user and user-defined members of its team (if applicable).

Each user entity has designated administrators who authorize team member access to information uploaded to Miro boards. User uploaded or created content is always owned by the customers. Access to production servers with databases storing customer data is restricted to a limited number of IT Operations Management personnel with credentials to access such data. All access to production environment is logged and monitored online. Miro employees cannot access user boards or see board content without customer approval.

The transmission, movement, and removal of information is restricted to authorized users and processes, and is protected during the same processes, enabling Miro to meet its commitments and requirements as they relate to security, availability, and confidentiality.

Processes and Procedures

Management has developed and communicated procedures to guide the provision of the organization's services. Changes to procedures are performed annually and authorized by management. These procedures cover the following key security life cycle areas:

- Data classification
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response
- Maintenance of restricted access to system configurations, user functionality, master passwords, powerful utilities, and security devices

SECTION B:
PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Regulatory Commitments

The organization is subject to General Data Protection Regulation (GDPR) and California Consumer Protection Act (CCPA) privacy regulations. The organization designs its security programs and business operations to maintain compliance with industry expectations and regulatory commitments. Miro's Data Processing Addendum outlines its commitments to comply with GDPR and CCPA. The organization's Master Service Agreement (MSA) notes the organization provides a platform for clients to provide data but does not process personally identifiable information (PII), PHI, PCI, or other restricted information. Regulatory responsibility is passed onto clients for data hosted in the Miro environment.

Contractual Commitments

The organization uses Master Cloud Agreements (MCAs) and public-facing documents to define agreed-upon services, terms, and conditions with its clients. Service-level agreements (SLAs) are included within MCAs. The only SLA Miro offers to its Enterprise Customers is the customer support response SLA. This option can be chosen with an additional fee.

System Design

Miro designs its online collaborative whiteboard platform system to meet its regulatory and contractual commitments. These commitments are based on the services that Miro provides to its clients, the laws and regulations that govern the provision of those services, and the financial, operational, and compliance requirements that Miro has established for its services. Miro establishes operational requirements in its system design that support the achievement of its regulatory and contractual commitments. These requirements are communicated in Miro's system policies and procedures, system design documentation, and contracts with clients.