RealtimeBoard, Inc. dba 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 December 1, 2021 through November 30, 2022.

KirkpatrickPrice

4235 Hillsboro Pike
Suite 300
Nashville, TN 37215

TABLE OF CONTENTS

ASSERTION OF REALTIMEBOARD, INC. DBA MIRO MANAGEMENT

ASSERTION OF REALTIMEBOARD, INC. DBA MIRO MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within RealtimeBoard, Inc. dba Miro’s online collaborative whiteboard platform system (system) throughout the period December 1, 2021, to November 30, 2022, to provide reasonable assurance that RealtimeBoard, Inc. dba 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 December 1, 2021, to November 30, 2022, to provide reasonable assurance that RealtimeBoard, Inc. dba 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*). RealtimeBoard, Inc. dba 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 December 1, 2021, to November 30, 2022, to provide reasonable assurance that RealtimeBoard, Inc. dba Miro’s service commitments and system requirements were achieved based on the applicable trust services criteria.

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

Andrey Khusid
Chief Executive Officer
RealtimeBoard, Inc. dba Miro
525 Brannan Street, Suite 100
San Francisco, CA 94107

Scope

We have examined RealtimeBoard, Inc. dba Miro's accompanying assertion titled "Assertion of RealtimeBoard, Inc. dba Miro Management" (assertion) that the controls within RealtimeBoard, Inc. dba Miro's online collaborative whiteboard platform system (system) were effective throughout the period December 1, 2021, to November 30, 2022, to provide reasonable assurance that RealtimeBoard, Inc. dba 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

RealtimeBoard, Inc. dba 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 RealtimeBoard, Inc. dba Miro's service commitments and system requirements were achieved. RealtimeBoard, Inc. dba Miro has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, RealtimeBoard, Inc. dba 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 RealtimeBoard, Inc. dba 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 RealtimeBoard, Inc. dba 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 RealtimeBoard, Inc. dba Miro’s online collaborative whiteboard platform system were effective throughout the period December 1, 2021, to November 30, 2022, to provide reasonable assurance that RealtimeBoard, Inc. dba 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

December 12, 2022

REALTIMEBOARD, INC. DBA MIRO’S DESCRIPTION OF ITS ONLINE COLLABORATIVE WHITEBOARD PLATFORM SYSTEM

SECTION A:
REALTIMEBOARD, INC. DBA MIRO'S DESCRIPTION OF THE BOUNDARIES OF ITS ONLINE COLLABORATIVE WHITEBOARD PLATFORM SYSTEM

Services Provided

RealtimeBoard, Inc. dba Miro (Miro) offers an online collaborative whiteboard platform that enables remote team users to add pictures, mock-ups, drawings, videos, sticky notes, office documents, and Google Drive files on an endless canvas and collaborate regardless of their location.

Miro's basic tools include the following:

- Whiteboarding tools: sticky notes, freehand drawing, shapes, links, texts, and presentation mode
- Collaboration tools: real-time collaborative editing, comments, text chat, voice and video chat, screen sharing, and 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, and 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 use marketing engines and software resellers to generate sales leads. Sales processes are tracked through Salesforce. Once sales 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.

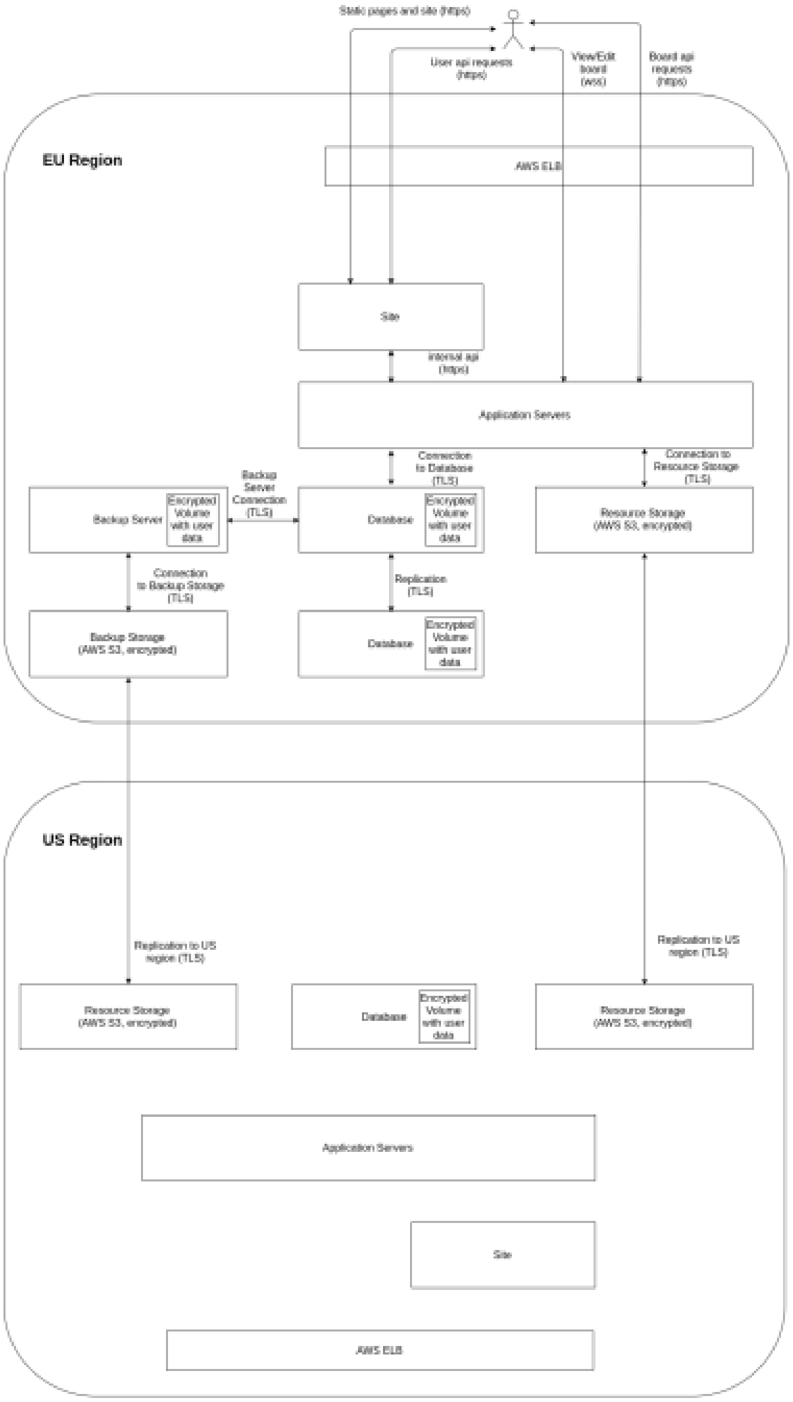
The onboarding team creates an account in the Gainsight customer service management (CSM) tool, which is used to manage the implementation. The support team creates the client profile and team account and enters the number of licenses purchased. Client queues and workflows are created in the Zendesk 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

Miro maintains a system inventory that tracks all devices within the organization’s environment. The inventory documents each device’s name, type, the providing vendor, function, OS, and any associated notes, including which employees is assigned to the device.



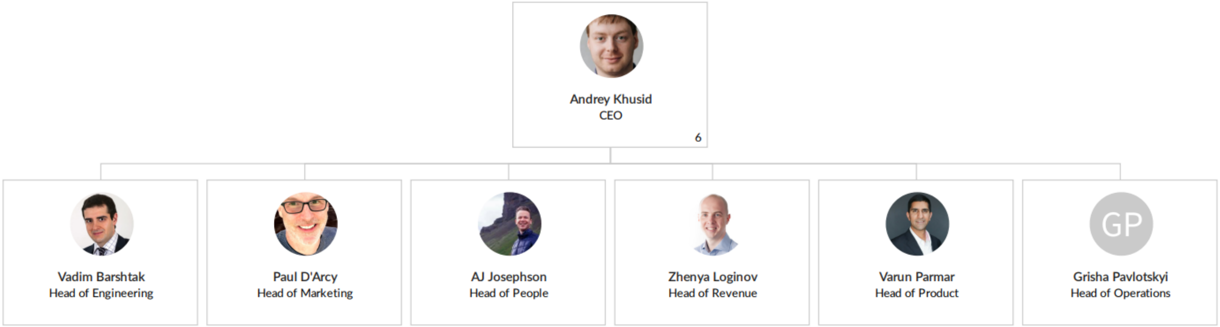
Static pages and site (https)
User api requests (https)
View/Edit board (wss)
Board api requests (https)
EU Region
AWS ELB
Site
internal api (https)
Application Servers
Connection to Database (TLS)
Connection to Resource Storage (TLS)
Backup Server
Encrypted Volume with user data
Backup Server Connection (TLS)
Database
Encrypted Volume with user data
Resource Storage (AWS S3, encrypted)
Connection to Backup Storage (TLS)
Replication (TLS)
Backup Storage (AWS S3, encrypted)
Database
Encrypted Volume with user data
US Region
Replication to US region (TLS)
Replication to US region (TLS)
Resource Storage (AWS S3, encrypted)
Database
Encrypted Volume with user data
Resource Storage (AWS S3, encrypted)
Application Servers
Site
AWS ELB

Software

The organization maintains a system inventory that lists both physical and virtual devices. Miro also maintains a critical software inventory that lists the software Miro uses to conduct its operations and provide its services. Software used includes the third-party payment application, Stripe.com. Credit card information is not stored or processed by Miro itself.

People

Miro is a private corporation that is owned by a series of investors. Miro is structured as a traditional hierarchy and is divided into business units that are managed by department heads who report to the CEO who, in turn, reports to the board of directors. Governance and oversight activities for Miro are performed by the board of directors. The board meets quarterly and consists of investor representatives, the CEO, and independent members. Miro's leadership structure is depicted on the following diagram.



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 user. This confidential and private information is available only to the user and user-defined members of its team (if applicable). Prohibited data, such as protected health information (PHI), cardholder data (CHD), special categories of data enumerated under GDPR, and IP, is not permitted on the Miro platform. Clients are made aware of this through MCAs. The organization maintains a privacy policy that addresses how the organization handles personal information according to relevant legislation and regulations.

Miro's Data Protection Policy specifies the organization's data retention policies, and the organization retains data according to these policies. The Data Protection Policy also specifies that Miro classifies data into four classes, each of which requires a different level of protection. Data classifications include the following:

- Unclassified public
- Copywrite
- Confidential
- Company private

- Client private sensitive
- Trade secrets

While in Miro’s systems, data is secured using restricted access, firewalls, a virtual private network (VPN), multi-factor authentication (MFA), unique user IDs, complex passwords, and encryption. Data at rest is encrypted using AES 256-bit encryption, and data in transit is encrypted using Transport Layer Security (TLS) 1.2. Data transmissions are conducted over secured HTTPS connections with TLS 1.2 encryption or through Prisma Access VPN tunnels that use IPsec with AES-256 cipher-block chaining (CBC) encryption and SHA-256 authentication. A VPN is required when remotely accessing systems and data.

Miro has established a process for securely managing encryption keys. Encryption keys are managed using secure encryption key management systems. Amazon Web Services (AWS) Key Management Service (KMS) is used to manage encryption keys for AWS tools. The organization manages encryption keys for the VPN, EC2 instances with Elastic Block Store (EBS), backup encryption, BitLocker, FileVault, and HTTPS/TLS systems through the native key management systems for each of those tools and systems. The Director of Trust and Reputation and the Infrastructure Team Lean are dually responsible for managing encryption keys.

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

Miro 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 the organization's commitment to comply with GDPR and CCPA. Regulatory responsibility is passed onto clients for data hosted in the Miro environment.

Contractual Commitments

Miro is committed to maintaining the security, availability, and confidentiality of client data. These commitments are communicated to clients through master cloud agreements (MCAs) and service-level agreements (SLAs). Miro uses MCAs and public-facing documents to define agreed-upon services, terms, and conditions with its clients. SLAs define Miro's service commitments and availability percentages; SLAs are defined in MCAs. Vendors are informed of Miro's confidentiality requirements through mutual non-disclosure agreements (MNDAs) that are executed prior to the beginning of a business engagement.

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.