Proprietary & Confidential

System Description of the Asana Service

SOC 3

Relevant to Security, Availability, and Confidentiality

FEBRUARY 1, 2021 TO JANUARY 31, 2022

MOSSADAMS

Table of Contents

I. Independent Service Auditor's Report

MOSSADAMS

Asana
633 Folsom Street, Suite 100
San Francisco, CA 94107

To the Management of Asana:

Scope

We have examined Asana's accompanying assertion in Section II titled "Asana's Assertion" (assertion) that the controls within the Asana Service (system) were effective throughout the period February 1, 2021 to January 31, 2022, to provide reasonable assurance that Asana'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*).

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

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Asana, to achieve Asana's service commitments and system requirements based on the applicable trust services criteria. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

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

- 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 Asana'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 Asana's service commitments and system requirements based the applicable trust services criteria

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

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 Asana's Asana Service were effective throughout the period February 1, 2021 to January 31, 2022, to provide reasonable assurance that Asana's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Moss Adams LLP

San Francisco, California
March 25, 2022

II. Asana's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within the Asana Service (system) throughout the period February 1, 2021 to January 31, 2022 to provide reasonable assurance that Asana'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 III titled "Asana's Description of the Boundaries of Its Asana Service" 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 February 1, 2021 to January 31, 2022, to provide reasonable assurance that Asana'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)*. Asana'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 III titled "Asana's Description of the Boundaries of Its Asana Service".

Asana uses a subservice organization for the management and hosting of production servers and databases. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Asana, to achieve Asana's service commitments and system requirements based on the applicable trust services criteria. The description presents the types of complementary subservice organization controls assumed in the design of Asana's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Asana, to achieve Asana's service commitments and system requirements based on the applicable trust services criteria. The description presents complementary user entity controls assumed in the design of Asana's controls.

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 February 1, 2021 to January 31, 2022, to provide reasonable assurance that Asana's service commitments and system requirements were achieved based on the applicable trust services criteria.

III. Asana's Description of the Boundaries of Its Asana Service

A. System Overview

1. Services Provided

COMPANY OVERVIEW

Asana provides a work management platform empowering teams to do great things together. With a mission of helping humanity thrive by enabling all teams to work together effortlessly, Asana seeks to eliminate the 'work about work' so that companies can focus on the work making the greatest impact.

Asana was founded in 2008 and is headquartered in San Francisco, CA. More than 100,000 paying organizations and millions of customers around the world, including Fortune 500 companies, use Asana to drive clarity of plan, purpose, and responsibility across their teams. Asana is available in 195 countries and 13 global languages.

SYSTEM DESCRIPTION

Asana provides a cloud-based application "Asana Service" to help customers effectively collaborate, organize, manage, coordinate, and complete work — from projects to processes.

Asana allows teams to break goals and ideas down into actionable tasks, assign those tasks, and communicate to move the work forward. Teams can use Asana to track anything, from bugs to leads to job applicants. By making plans, responsibilities, and deadlines clear, Asana empowers and enables teams to deliver great results.

2. System Boundaries

The system boundaries for consideration within the scope of this report are the processes, systems, and software that store, access, operate, or transmit customer data within Asana. Specifically, the system environment includes the management of the provider hosting the network, production and staging servers, the Asana production support workstations, and the personnel who support the system.

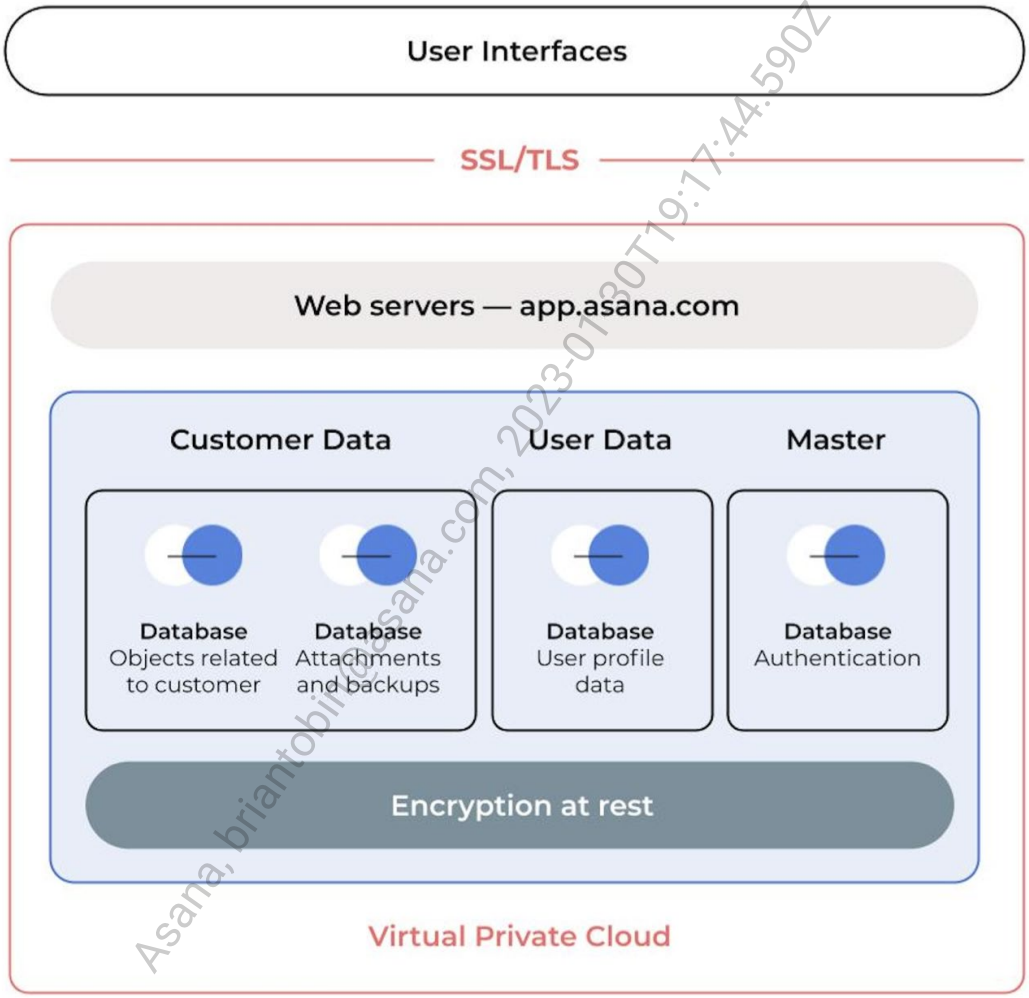
3. Subservice Organizations

The scope of this report includes only the controls Asana directly executes and excludes controls that are the responsibility of Asana's subservice organization. Specifically, Asana has a contract with Amazon Web Services (AWS) and monitors AWS' compliance with regard to security, availability, and confidentiality. The controls expected to be in place at AWS are identified in the subsequent section titled Complementary Subservice Organization Controls (CSOC).

4. Infrastructure

Asana utilizes cloud computing service offerings, primarily from AWS, as the core building blocks of the Asana Service. AWS manages the security and compliance of the cloud computing infrastructure, and Asana manages the security and compliance of the software and sensitive data residing in the cloud computing infrastructure.

Asana has designed the network architecture to be secure, scalable, and easily managed using the networking services and building blocks AWS provides.



5. Software

The Asana Service is a web-based software-as-a-service application. The services and components comprising the Asana Service are primarily written in JavaScript, Typescript, Python, and Scala based on the React application framework.

6. People

The following outlines the various teams and functions who support the Asana environment:

- Communications / Public Relations
- Sales & Customer Success
- Information Technology (IT)
- Infrastructure Engineering
- Legal
- People Ops (HR)
- Product
- Product Engineering
- Security
- User Operations

7. Data

Asana designs its processes and procedures to protect customer data. For the interests of this report, two key categories of customer data are considered:

CUSTOMER DATA

'Customer Data' is defined as information submitted by an end user through the Asana Service, including the associated messages, attachments, files, tasks, project names, team names, channels, conversations, and other similar content. This data is typically entered in the core Asana UI as Asana tasks, projects, teams, or attachments. A business entity could generally consider this data as intellectual property of the business.

CUSTOMER PERSONAL DATA

Customer Personal Data is defined as non-sensitive personal data about a user in Asana, such as names, email addresses, or roles. This data is typically entered through Asana's "My Profile Settings" dialog. Note: Asana does not solicit sensitive personal data, such as social security numbers, to be uploaded into the system.

8. Processes and Procedures

Asana maintains a set of policies that are published and communicated to Asana personnel on the intranet. The following policies are relevant to the scope of this report:

- Asset Management Policy
- Change Management Policy
- Data Classification Policy
- Data Access Policy
- Employee Handbook (including the Code of Conduct)
- Incident Response Plan

- Information Security & Data Protection Policy
- Privacy Statement
- Risk & Vulnerability Management Policy

Asana requires each employee or contractor performing services for Asana to sign the Information Security & Data Protection Policy or the Asana Services Agreement, which outline the company's policies and expectations with respect to the following:

- Access to and handling of confidential customer and company information ("confidential information")
- Reporting of known or suspected security breaches
- Internet and email security expectations
- Use of passwords on computers and mobile devices
- Physical security standards for computers, mobile devices, and facilities

Asana's security policies and approach is documented and communicated to clients on its Trust Portal (https://asana.com/trust), Terms of Service, and other related agreements. Asana's security strategy covers various aspects of its business, including:

- Asana corporate security policies
- Data model access control in Asana
- Operational security processes
- Physical and environmental security
- Scalability and reliability of Asana's system architecture
- Service development and maintenance
- Systems development and maintenance
- Working with third-party security experts

Asana establishes operational requirements to support the achievement of its security, availability, and confidentiality commitments, and other system requirements. Such requirements are communicated in Asana's system policies and procedures, system design documentation, and contracts with customers. Information security policies define the organization-wide approach to how systems and data are protected. Collectively, these documents 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 Asana Service.

B. Principal Service Commitments and System Requirements

Asana designs its processes and procedures to protect customer data. Asana security commitments are documented and communicated to customers in the Terms of Service, subscriber agreements, addendums, other related agreements, and in the description of services provided online. These security commitments are standardized and include the following:

- Protecting customer data
- Encrypting data in transit and storage
- Limiting access to customer data

C. Complementary Subservice Organization Controls

Asana's controls related to the Asana Service cover only a portion of overall internal control for each user entity of Asana. It is not feasible for the criteria related to the Asana Service to be achieved solely by Asana. Therefore, each user entity's internal controls must be evaluated in conjunction with Asana's controls, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Complementary Subservice Organization Controls	
1	Access to hosted systems requires strong authentication mechanisms.
2	New and existing user access and permissions to hosted systems are approved by appropriate personnel prior to being granted.
3	Terminated user access permissions to hosted systems are removed in a timely manner.
4	User access permissions to hosted systems are reviewed by appropriate personnel on a regular basis.
5	Privileged access to hosted systems and the underlying data is restricted to appropriate users.
6	Access to the physical facilities housing hosted systems is restricted to authorized users.
7	Production media is securely decommissioned and physically destroyed prior to being removed from the data center.
8	Network security mechanisms restrict external access to the production environment to authorized ports and protocols.
9	Connections to the production environment require encrypted communications.
10	Anti-virus or anti-malware solutions detect or prevent unauthorized or malicious software on hosted systems.
11	System configuration changes are enforced, logged, and monitored.
12	Hosted systems are scanned for vulnerabilities. Any identified vulnerabilities are tracked to resolution.
13	System activities on hosted systems are logged, monitored and evaluated for security events. Any identified incidents are contained, remediated and communicated according to defined protocols.

Complementary Subservice Organization Controls	
14	Access to make changes to hosted systems is restricted to appropriate personnel.
15	Changes to hosted systems are documented, tested, and approved prior to migration to production.
16	Personnel monitor processing and system capacity on hosted systems.
17	Personnel execute and monitor daily backups. Any identified errors are resolved in a timely manner.
18	Environmental mechanisms provide protection over fire, water, power outages, temperature changes and natural disasters.
19	Software and recovery infrastructure are implemented over hosted systems.

D. Complementary User Entity Controls

Asana's Asana Service was designed under the assumption that certain controls would be implemented by the user entities for whom it provides its Asana Service. In these situations, the application of specific controls at these customer organizations is necessary to achieve certain criteria included in this report.

This section describes additional controls that should be in operation at the customer organizations to complement the controls at Asana. User auditors should consider whether the following controls have been placed in operation by the customers.

Each customer must evaluate its own internal control structure to determine if the identified customer controls are in place. Users are responsible for:

Complementary User Entity Controls	
1	Configuring appropriate password settings based on available password settings that include SAML and single sign-on.
2	Granting, removing, and reviewing access to their Asana environment.
3	Ensuring the data entered into their Asana environment is appropriate based on their data classification requirements.

MOSSADAMS