Report on Asana's Service Relevant to Security, Availability, and Confidentiality (SOC 3 Report)

For the Period February 1, 2020 to January 31, 2021

THE cadence GROUP

O 801.349.1360
F 866.326.6612

PO Box 711190
Salt Lake City, Utah 84171
www.thecadencegroup.com

Section I – Report of Independent Service Auditors

To: Asana, Inc.

Scope

We have examined Asana's accompanying assertion, titled "Asana's Assertion" (assertion), that the controls within Asana's Service were effective throughout the period February 1, 2020 to January 31, 2021, 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).

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 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 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 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 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 are 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 policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Asana's system were effective throughout the period February 1, 2020 to January 31, 2021, 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.

Cadence Assurance LLC

March 11, 2021
Salt Lake City, Utah

Section II – Asana's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Asana's Service throughout the period February 1, 2020 to January 31, 2021, 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 Attachment 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 February 1, 2020 to January 31, 2021, 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 Attachment 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 February 1, 2020 to January 31, 2021, to provide reasonable assurance that Asana's service commitments and system requirements were achieved based on the applicable trust services criteria.

Asana, Inc.
March 11, 2021

Attachment A – Asana's Description of the Boundaries of its Asana Service

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 75,000 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 190 countries and 6 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.

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 service 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.

Subservice Organizations

Asana contracts with Amazon Web Services (AWS) to provide management and hosting of production servers and databases. The subservice organization has been excluded from the scope of this report; the controls they are expected to provide are included in Attachment D, titled *Complementary Subservice Organization Controls (CSOC).*

System Components

To deliver the Asana Service, Asana uses the following infrastructure, software, people, procedures, and data.

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. Please refer to the Shared Responsibility Model from AWS: https://aws.amazon.com/compliance/shared-responsibility-model/.

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

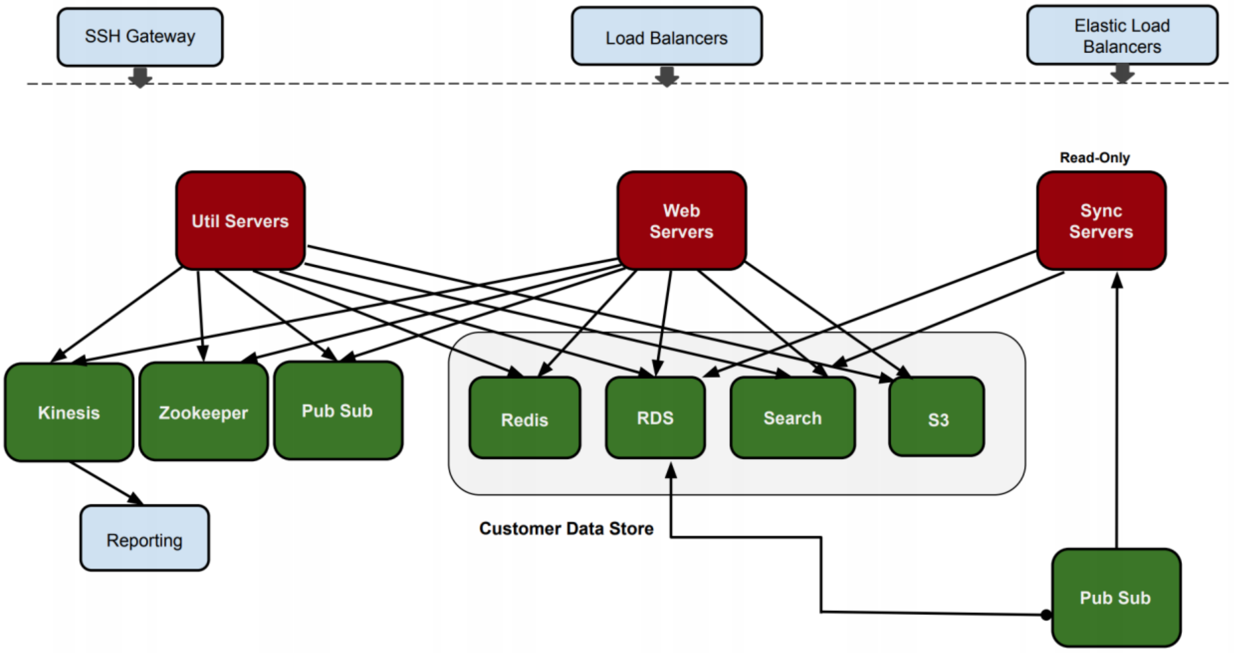

Figure: Asana Network Diagram

Software

The Asana Service is a web-based software-as-a-service application. The services and components comprising the Asana Service include:

- Threat Management
- Logging
- Monitoring
- Network Protection
- Intrusion Detection
- Vulnerability Testing and Vulnerability Management
- Change Management

People

Asana employees involved in the definition, development, operation, or support of the core Asana Service are grouped in the following primary areas:

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

Procedures

Asana maintains the following set of policies that are published and communicated to Asana personnel on the intranet:

- Asset Management Policy
- Change Management Policy
- Code of Conduct
- Data Classification Policy
- Employee Handbook
- Incident Response Policy
- Information Security Policy
- Privacy Policy
- Risk Management Policy

Asana's security policies and approach is documented and communicated to clients on its Trust page (https://asana.com/trust), addendums, and other related agreements, as well as in the description of services provided online.

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.

Data

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

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.

Asana's Information Security Management Program restricts access to Customer Data and Customer Personal Data to those employees who are required to access such data as a part of their job and then only in those circumstances where access to such data is required to provide a specific service. In such circumstances, the employee is directed to access only the minimum amount of Confidential Data or Customer Personal Data necessary to perform the task at hand.

The Information Security Management Program requires legal requests for information (e.g., any law enforcement requests, subpoenas, or court documents) to be forwarded immediately to the Legal team for handling in accordance with Asana's Law Enforcement Guidelines, which can be found at: https://asana.com/terms#law-enforcement-guidelines.

Internal Control Framework

Asana has adopted a control framework to meet its security, availability, and confidentiality commitments. This framework includes the following aspects: control environment, risk assessment, control activities, information and communication, and monitoring.

Additionally, 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. See Attachment C for identified complementary user entity controls.

Control Environment

The control environment at Asana is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment include integrity and ethical values, management participation, Asana's organizational structure, the assignment of authority and responsibility, commitment to competence, and accountability.

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Asana's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Asana's ethical and behavioral standards, how they are communicated, and how they are reinforced in practice.

Asana's control consciousness is influenced significantly by the values and behavioral standards communicated by management to personnel through policy statements, codes of conduct, and shared mission and value statements. Management takes actions to create an environment that emphasizes taking and giving full responsibility, focusing on Asana's mission, and clarifying who's doing what, by when, how, and why. This culture creates an environment where employees take actions to maximize the success of Asana's mission, work with clear accountability, and have responsibility for their behavior and decisions.

Risk Assessment

Asana maintains its Risk Management Policy intended to proactively identify vulnerabilities within Asana systems, and assess new and emerging threats to company operations. Risk management personnel, comprised of members of the Security team, meet annually to discuss changes to external and internal factors that may impact or prevent Asana from meeting its objectives.

Asana's Security team records product-related risks in a risk register tracking identified risks, agreed-upon risk mitigation plans, and the status of risk mitigation activities.

Control Activities

Controls have been established to help ensure processes operate as intended to keep service data secure and confidential in the following areas:

- Vendor management
- Asset management
- Logical access security
- Network security
- Endpoint security
- Data encryption
- System monitoring
- Vulnerability management
- Incident management
- Change management
- Backup and availability
- Disaster recovery and business continuity management
- Data Retention and Disposal

Information and Communication

To help align Asana business strategies and goals with operating performance, Asana is committed to maintaining effective communication with customers, vendors, and employees.

External Communications

Asana communicates with customers, vendors, and third-party partners through multiple channels. These channels include:

- Terms and policies: https://asana.com/terms
- Statement on security: https://asana.com/trust
- Webinars, blogs, and newsrooms
- Email
- Contractual documentation

Customers are specifically notified via email if there are changes to the Terms of Service, Privacy Policy, or Subscriber Agreement.

Internal Communications

Policies are updated as necessary and are reviewed and approved annually by assigned owners. Asana implements and maintains a program to train new personnel on security and privacy responsibilities. Personnel complete training within their first month of employment and annually thereafter. IT maintains appropriate documentation that personnel have completed the training and agree to the related policies.

Security and Legal teams annually present security and privacy updates identified from external assessments, internal monitoring, and internal controls to the executive leadership team and the board of directors. The Security team also implements and maintains an ongoing training program for Asana personnel with access to Asana systems. The ongoing training program includes, at a minimum: (a) alerts communicating new security developments; (b) periodic reminders reinforcing current security policies and procedures; and (c) annual security refresher courses.

Monitoring

Asana has developed a suite of controls to monitor the compliance of its control environment. These controls are designed to be complimentary to Asana's existing suite of controls and include user access reviews, code change reviews, security group reviews, vendor reviews, and internal control assessments.

Attachment B – Principal Service Commitments and System Requirements

Asana designs its policies, procedures, and processes to help ensure security, availability, and confidentiality commitments to customer service data. Asana commitments are documented and communicated to customers in contractual documentation, terms agreements, and the Trust page located on the Asana website.

Asana has adopted a control framework to meet its commitments. This framework includes the following aspects: control environment, risk assessment, control activities, information and communication, and monitoring outlined in Attachment A.

Attachment C – Complementary User Entity Controls

Asana's controls were designed under the assumption that certain controls would be implemented by user organizations, the application of which is necessary to meet certain trust services criteria identified in this report. This section highlights those internal control responsibilities Asana believes should be present at each customer, and has considered in developing its controls reported herein. Asana customers should evaluate their own control environment to assess if the following controls are implemented and operating effectively. These complementary user entity controls do not represent a comprehensive list of controls that should be employed by Asana customers, but provide a summary of controls necessary to meet the stated trust services criteria presented in this report. These controls include the following:

- Customers utilizing single sign-on or SAML for authentication are responsible for ensuring appropriate password configuration.
- Customers are responsible for granting, removing, and reviewing access to their Asana environment.
- Customers are responsible for ensuring the data entered into their Asana environment is appropriate based on their data classification requirements.

Attachment D – Complementary Subservice Organization Controls

Asana contracts with Amazon Web Services (AWS) to provide management and hosting of production servers and databases. Controls managed by this third-party subservice provider are not included in the scope of this report. Expected subservice provider controls that have an effect on specific criteria include the following:

- Access to hosted systems requires strong authentication mechanisms.
- New and existing user access and permissions to hosted systems are approved by appropriate personnel prior to be granted.
- Terminated user access permissions to hosted systems are removed in a timely manner.
- User access permissions to hosted systems are reviewed by appropriate personnel on a regular basis.
- Privileged access to hosted systems and the underlying data is restricted to appropriate users.
- Access to the physical facilities housing hosted systems is restricted to authorized users.
- Production media is securely decommissioned and physically destroyed prior to being removed from the data center.
- Network security mechanisms restrict external access to the production environment to authorized ports and protocols.
- Connections to the production environment require encrypted communications.
- Antivirus or antimalware solutions detect or prevent unauthorized or malicious software on hosted systems.
- System configuration changes are enforced, logged, and monitored.
- Hosted systems are scanned for vulnerabilities. Any identified vulnerabilities are tracked to resolution.
- 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.
- Access to make changes to hosted systems is restricted to appropriate personnel.
- Changes to hosted systems are documented, tested, and approved prior to migration to production.
- Personnel monitor processing and system capacity on hosted systems.
- Personnel execute and monitor daily backups. Any identified errors are resolved in a timely manner.
- Environmental mechanisms provide protection over fire, water, power outages, temperature changes and natural disasters.
- Software and recovery infrastructure are implemented over hosted systems.