REPORT ON ASANA'S SERVICE RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY (SOC 3 REPORT)

FOR THE PERIOD FEBRUARY 1, 2019 TO JANUARY 31, 2020

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 system were effective throughout the period February 1, 2019 to January 31, 2020, 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.

THE cadence GROUP

O 801.349.1360
F 866.326.6612

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

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.

Service Auditor's Independence and Quality Control

We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA. We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

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, 2019 to January 31, 2020, 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 30, 2020
Salt Lake City, Utah

Section II – Asana's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Asana's system throughout the period February 1, 2019 to January 31, 2020, to provide reasonable assurance that Asana's service commitments and system requirements relevant to security, availability, and confidentiality, were achieved.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period February 1, 2019 to January 31, 2020, 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.

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, 2019 to January 31, 2020, to provide reasonable assurance that Asana's service commitments and system requirements were achieved based on the applicable trust services criteria.

Asana, Inc.
March 30, 2020

Section III – Asana's Description 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. It is available in 195 countries and 6 global languages.

System Description

Asana provides a cloud-based platform 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 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

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 entitled *Complementary Subservice Organization Controls (CSOC)*.

Principle 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, but are not limited to, the following:

- Protecting customer data
- Encrypting data transmissions and storage
- Limiting access to customer data

System Components

The following section outlines the system components that make up the Asana service.

Infrastructure

Asana utilizes cloud computing service offerings, primarily from Amazon Web Services (AWS), as the core building blocks of the Asana platform. 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.

Software

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

People

Asana teams and functions who support the Asana environment include Security, Product Engineering, Infrastructure Engineering, Product, Information Technology (IT), Legal, Communications / Public Relations, User Operations, Customer Success, and People Ops (HR).

Procedures

Asana maintains a set of policies that are published and communicated to Asana personnel. Policies are updated as necessary and are reviewed and approved.

The following policies are relevant to the scope of this report:

- Employee Handbook
- Confidential Information and Invention Assignment Agreement (CIIAA)
- Information Security Policy
- Code of Conduct
- Privacy Policy
- Change Management Policy
- Asana Risk Management Process

Asana requires each employee or contractor performing services for Asana to sign the Information Security Policy or the Contractor Service Agreement.

Asana's security policies and approach is documented and communicated to clients on its statement on security (https://asana.com/security-statement), 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 platform.

Data

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

Customer Data
'Customer Data' is defined as information submitted by an end user through the Asana platform, 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

The following section describes the aspects of Asana's internal control environment.

Control Environment

A company's internal control environment reflects the overall attitude, awareness, and importance of safeguarding information assets. The collective control environment encompasses management and employee efforts to establish and maintain an environment that supports the effectiveness of specific controls.

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.

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 an ongoing risk management process 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 also 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 implemented to address system and data risks. Controls have been designed and implemented in the following areas:

- Vendor management
- Asset management
- Logical access security
- Network security
- Encryption
- Endpoint security
- System monitoring
- Backup and availability
- Incident response
- Vulnerability management
- Customer data retention and disposal
- Disaster recovery and business continuity management
- Change management

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/security-statement
- 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

IT 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. IT also implements and maintains an ongoing training program for Asana personnel with access to Asana systems.

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.

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.

Monitoring control activities include weekly code validations, quarterly access reviews, annual vendor assessments, and an annual internal control evaluations.

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 are responsible for granting, removing, and reviewing access to their Asana environment (Common Criterion 6.2, Common Criterion 6.3).
- Customers are responsible for ensuring the data entered into their Asana environment is appropriate based on their data classification requirements (Confidentiality 1.1).

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 are included below.

Criteria	Expected Controls at AWS
CC6.1 – The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Access to hosted systems requires users to use a secure method to authenticate. User content is segregated and made viewable only to authorized individuals. Network security mechanisms restrict external access to the production environment.
CC6.2 – Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	New user accounts are approved by appropriate individuals prior to being provisioned. User accounts are removed when access is no longer needed. User accounts are reviewed on a regular basis by appropriate personnel.
CC6.3 – The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Access modifications to hosted systems are approved by appropriate individuals prior to being provisioned. User accounts are removed when access is no longer needed. User accounts are reviewed on a regular basis by appropriate personnel.
CC6.4 – The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Access to physical facilities is restricted to authorized users.
CC6.5 – The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and	Production media is securely decommissioned and physically destroyed prior to being removed from the data center.

Criteria	Expected Controls at AWS
software from those assets has been diminished and is no longer required to meet the entity's objectives.	
CC6.6 – The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Network security mechanisms restrict external access to the production environment. Encrypted communication is required for connections to the production system.
CC6.7 – The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Access to hosted data is restricted to appropriate users. Hosted data is protected during transmission through encryption and secure protocols.
CC6.8 – The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Antivirus or antimalware solutions are installed to detect or prevent unauthorized or malicious software.
CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	System configurations changes are logged and monitored. Vulnerabilities are identified and tracked to resolution.
CC7.2 – The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Security events are monitored and evaluated to determine potential impact per policy.
CC7.3 – The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Operations personnel log, monitor and evaluate to incident events identified by monitoring systems
CC7.4 – The entity responds to identified security incidents by executing a defined incident response program to understand, contain,	Operations personnel respond, contain and remediate incident events, and update stakeholders, as needed.

Criteria	Expected Controls at AWS
remediate, and communicate security incidents, as appropriate.	
CC8.1 – The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	System changes are documented, tested, and approved prior to migration into production. Access to make system changes is restricted to appropriate personnel.
A1.1 – The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	Operations personnel monitor processing and system capacity.
A1.2 – The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	Environmental controls protect the physical devices supporting the production environment.
A1.3 – The entity tests recovery plan procedures supporting system recovery to meet its objectives.	System failover and backup procedures are tested.