Atlassian PTY Ltd.

System Organization Controls (SOC) 3 Report

Atlassian Service Organization's Description of the Boundaries of Its Trello System

For the period November 1, 2018 through March 31, 2019

Management's Report of its Assertions on the Effectiveness of Its Controls over Trello Based on the Trust Services Criteria for Security, Availability, and Confidentiality

May 28, 2019

We, as management of, Atlassian Pty Ltd ("Atlassian") are responsible for:

- Identifying the Trello (System) and describing the boundaries of the System, which are presented in Attachment A
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system, which are presented in Attachment B
- Identifying, designing, implementing, operating, and monitoring effective controls over the Trello (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirements
- Selecting the trust services categories that are the basis of our assertion

We assert that the controls over the system were effective throughout the period November 1, 2018 to March 31, 2019, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, confidentiality set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Very truly yours,

DocuSigned by:
Tom Kennedy
D9F75B69402F4F6...

Tom Kennedy
Chief Legal Officer

Ernst & Young LLP
303 Almaden Boulevard
San Jose, CA 95110

Tel: +1 408 947 5500
Fax: +1 408 947 5717
ey.com

Building a better working world

Report of Independent Accountants

To the Management of Atlassian Pty Ltd.

Scope:

We have examined management's assertion, contained within the accompanying Management's assertion regarding the effectiveness of its controls over Trello based on the trust services criteria for security, availability, and confidentiality (Assertion), that Atlassian's controls over Trello (System) were effective throughout the period November 1, 2018 to March 31, 2019, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in the AICPA's TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

Management's Responsibilities

Atlassian's management is responsible for its assertion, selecting the trust services categories and associated criteria on which the its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the Trello (System) and describing the boundaries of the System
- Identifying our principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system
- Identifying, designing, implementing, operating, and monitoring effective controls over the Trello (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirements

Our Responsibilities

Our responsibility is to express an opinion on the Assertion, based on our examination. 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. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Atlassian's relevant security, availability, and confidentiality policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including

Ernst & Young LLP
303 Almaden Boulevard
San Jose, CA 95110

Tel: +1 408 947 5500
Fax: +1 408 947 5717
ey.com

Building a better working world

an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Atlassian's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Inherent Limitations

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve Atlassian's principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Opinion

In our opinion, Atlassian's controls over the Trello system were effective throughout the period November 1, 2018 to March 31, 2019, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria.

Restricted Use

This report is intended solely for the information and use of Atlassian and user entities of Atlassian's Trello system and is not intended to be, and should not be, used by anyone other than these specified parties.

Ernst & Young LLP

San Jose, California
May 28, 2019

Attachment A – Atlassian Service Organization's Description of the Boundaries of Its Trello System

Company Overview and Background

Atlassian was founded in 2002 by Scott Farquhar and Mike Cannon-Brookes. Atlassian had its Initial Public Offering ("IPO") in 2015. Atlassian has offices in San Francisco and Mountain View, California, New York, Sydney, Australia, Manila, Philippines, Yokohama, Japan, Amsterdam, Netherlands, Austin, Texas, Boston, Massachusetts, Falls Church, Virginia, Ankara, Turkey, and Bengaluru, India.

Atlassian's mission is to unleash the potential in every team. Its collaboration software helps teams organize, discuss and complete shared work. Teams of more than 65,000 staff, as well as large and small organizations use Atlassian's project tracking, content creation and sharing, real-time communication, and service management products to work better together and deliver quality results on time. Atlassian products include Jira Software, Jira Service Desk, Confluence, Bitbucket, Trello, and Opsgenie.

The system in-scope for this report is primarily the Trello system hosted at Amazon Web Services ("AWS") and the supporting IT infrastructure and business processes. This report does not include add-ons, marketplace applications, plugins, and billing services.

Overview of Products and Service

Trello is a visual collaboration tool that creates a shared perspective on any project. Trello helps teams to get a shared perspective on projects through a system of boards, lists, and cards. Trello lets teams organize and prioritize personal lives and work in a fun, flexible, and rewarding way. Trello is available to teams via web or dedicated apps across desktop and mobile platforms.

Infrastructure

Trello is hosted at Amazon Web Services ("AWS") data centers, using the AWS Infrastructure as a Service offering ("IaaS"). The services that make up the Trello system are primarily isolated within a single large private network, which is spread out across up to 5 failure domains (or Availability Zones) for redundancy and fault-tolerance.

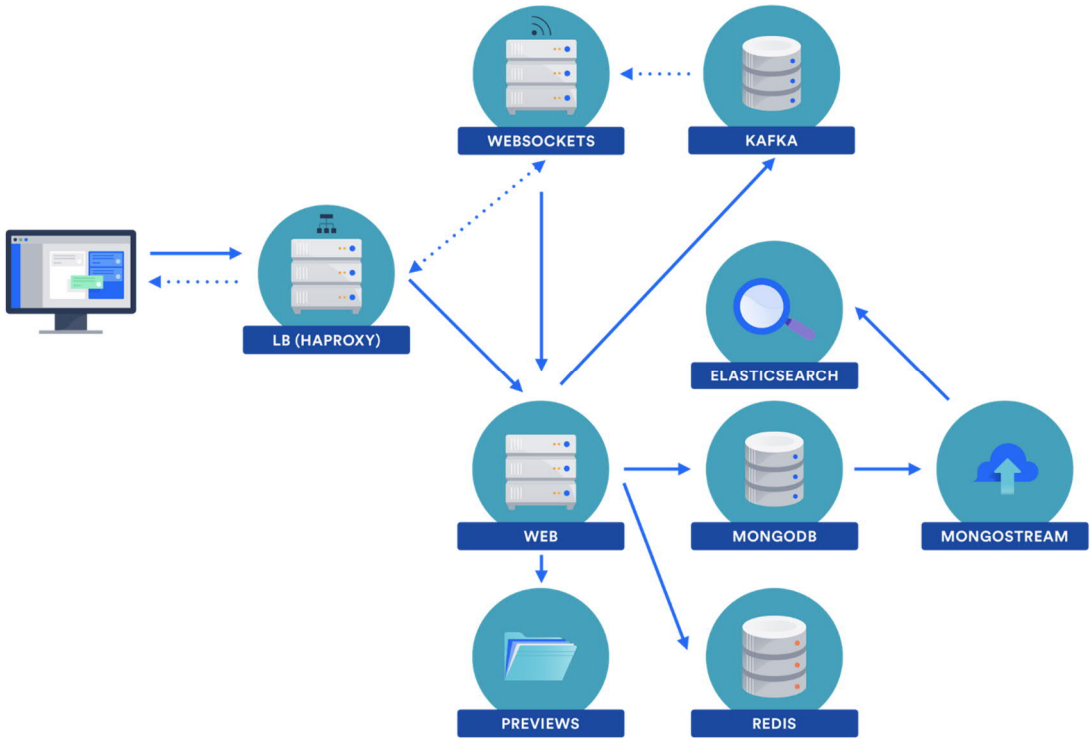

Figure 1: Trello's Infrastructure

The core application is composed of the following 5 services within Atlassian's network:

- Data Storage: MongoDB, which is hosted on services in AWS, is used to store customer data within Trello.
- Messaging Queue and Delivery: Kafka is a message queue solution used within Trello to facilitate real-time updates. Updates are propagated to appropriate users via the Web Socket Service.
- Load Balancers and Network Connections: HAProxy is used as the load balancer to ensure that incoming traffic is properly sorted by type and evenly distributed amongst application nodes. Akamai is used to terminate customers' HTTPS connections, as well as connect customers to the API and web socket services via local POPs.
- Indexing of Data: ElasticSearch is used for indexing data for the purposes of Search.
- Data Caching: Redis is used for data caching and lookups.

The load balancers and Redis are out of scope for this report. Only the messaging queue services, access to the database, and backups of customer data are in scope for this report.

The processes and controls managed by AWS are excluded from the scope of this report.

Servers

AWS provides Infrastructure as a Service ("IaaS") and the initial creation of the virtual servers, which run Trello. However, the software and operating system configurations are managed by Atlassian's Trello team using a configuration management system (Puppet).

Database

Trello's primary datastore is a MongoDB cluster within the private network, which is hosted in AWS and managed by the Trello Systems Team. The MongoDB cluster is sharded and its nodes are spread out of a minimum of 3 Availability Zones for fault-tolerance and redundancy.

Search indexes are stored within an ElasticSearch cluster, which is also managed by the Trello team, and hosted within the private network on AWS.

User attachments are stored within Amazon S3 to increase durability guarantees, and to segregate attachments using a unique identifier that is stored in the Trello database. The unique identifier ties the file objects to the user, as well as the board or card the attachment was uploaded to.

The data in all the above cases is encrypted at rest.

Software

The following software, services, and tools support the Trello control environment and are in scope as part of the controls and processes being executed:

- Akamai – Global edge; DDoS mitigation and reverse proxy
- ElasticSearch – Indexing of data
- AWS Glacier - Data archiving and long-term backup storage service
- AWS S3 - Stores attachments and customer data backups for Trello
- Bamboo – Bamboo is Atlassian's developed continuous integration tool used to perform automated testing and deployment activities
- Bitbucket Cloud – Atlassian's developed source code and development projects tool
- Centrify – Single sign on service used for Atlassian
- GoogleAuth - Single sign on service used for Atlassian
- Google Cloud Storage ("GCS") – Redundant offsite backup storage location
- Help Scout – Customer support tool
- Impraise – performance feedback tool
- Jira - Ticketing system used for incident management, user access provisioning, and change management process.
- Kafka – Message queue service
- Lever – Hiring tool
- Nagios – System monitoring and alerting platform
- Nexpose - Vulnerability scanning tool
- PagerDuty – Alerting tool for monitoring of availability

- Puppet - open-source software configuration management tool
- Slack - Collaboration or instant messaging tool
- SparkPost – Outgoing email service provider
- Splunk – Monitoring of security and availability tool
- SQS - Message queue service managed by AWS
- Trello – Used for development, backlog planning, execution, and team coordination
- Trello Admin Panel - Internal tool used by Trello staff to support customers; including impersonation
- Workday – Human Resource (HR) system

AWS, GCS, Akamai, and SparkPost are managed by third-party vendors. Atlassian performs a review of the SOC 2 reports for these vendors. The evaluation of the SOC 2 report is performed and reviewed by the Risk and Compliance Team, which includes an assessment of complementary user entity controls, subservice organizations, and mapping of the controls to key risks. If there are exceptions, Atlassian will review the severity and impact of the exceptions, and if needed, follow up with the individual vendor. Centrify, GoogleAuth, Help Scout, Impraise, Lever, PagerDuty, Slack, SQS, and Workday are managed by third-party vendors; however, customer data is not stored in these applications. These are supporting and monitoring tools, and are only applicable to support certain controls and criteria.

Vendor agreements, including any security, availability, and confidentiality commitments, are reviewed by appropriate Atlassian management during the procurement process. Prior to services rendered, the vendor and Atlassian are required to sign the vendor agreement terms and conditions.

Data

Customers can sign up for Trello using the www.trello.com website or via Trello's mobile apps. Upon accepting the terms and conditions, and completing the sign-up flow, a new database record and unique identifier are created in MongoDB for that customer account. The unique ID is used thereafter for associating data with the specific user account. The data is logically separated from other users' data using these unique ID's. All user created data are similarly assigned unique identifiers such that they can be correctly associated to users, teams, enterprises, and so on.

Customers whose accounts are provisioned from an external enterprise single sign-on solution follows the same process as non-SSO accounts except for the one-time import of the customers' personal details from the external identity provider. Customers are responsible for the security and confidentiality of the data prior to the import.

All production customer data is encrypted at rest within Atlassian's network, which is managed by AWS. AWS' SOC 2 report is reviewed at least annually by Atlassian. External users connect to Trello using encryption via the SSL (TLS) protocol. Additionally, there is no production data residing in the non-production environments.

Organizational Structure

Atlassian's organizational structure is managed by a committee consisting of Human Resources, Financial Planning and Analysis, as well as Senior Management and Leadership (including the Co-Founders).

The following organizational chart identifies the teams responsible for human resources, strategic planning, education/training, legal matters, business growth/modeling, finance, accounting, and technology operations:

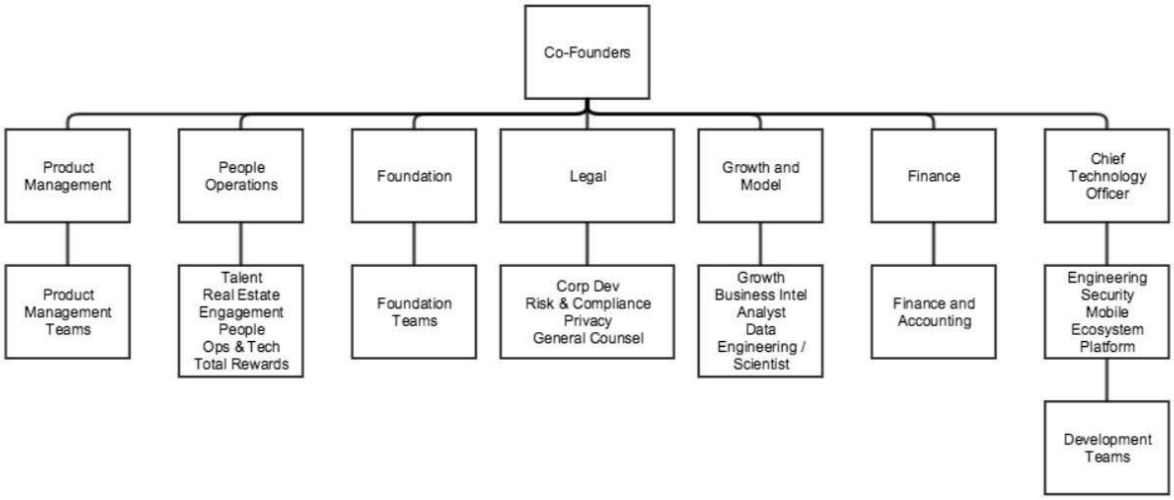

Figure 2: Atlassian's Organizational Chart

The organizational charts are reviewed by appropriate Atlassian management and updated semi-annually. Additionally, organizational charts are automatically updated based on employee action notices and is available to all Atlassian employees via Atlassian's HR system, Workday.

The Co-Founders are responsible for directing all designated areas including Product Management, People Operations, Foundation, Legal, Growth and Modeling, and the Technology teams. All teams have full responsibility over key operations within Atlassian:

- Product Management - focuses on validating the demands of customers, provides insight and guidance around minimum viable product and user experience.
- People Operations (in partnership with the people leaders) - focuses on determining the right talent strategy to deliver against the needs of Atlassian. People team is responsible for talent acquisition and learning, total rewards and technology, and workplace experiences.
- Foundation - Exists to harness the resources of Atlassian to champion organizations who believe that education is the key to eliminate disadvantage. This is accomplished by improving educational outcomes in developing countries, increasing skill-based volunteering and leveraging Atlassian's products.

- Legal - responsible for matters related to corporate development, privacy, general counsel operations, public relations, risk and compliance.
- Growth and Model - responsible for monitoring business trends, analytics, data engineering and data science.
- Finance - responsible for handling finance and accounting
- Chief Technology Officer (Technology Operations) - oversees Engineering, Security, Mobile, Ecosystem and Platform.
    - Head of Engineering, Software Teams oversees all operations for the products.
    - Development Manager:
        - Drives and improves product quality and innovation, team productivity, manages simultaneous projects in an agile fashion, customer satisfaction and product supportability.
        - Coordinate multiple streams of software development, involving multiple teams, geographic distribution and indirect reports
        - Collaborate with Product Management by contributing to roadmaps, setting priorities, and providing estimates
        - Collaborate with Customer Support to help ensure customer success and drive quality improvements
        - Promote, define, refine and enforce best practices and process improvements that fit Atlassian's agile methodology
        - Provide visibility through metrics and project status reporting
        - Set objectives for people and teams and holds them accountable
        - Work with Recruitment to attract and hire outstanding individuals to create high performing balanced teams
        - Lead by example and practice an inclusive management style.

Policies and Procedures

Atlassian maintains a Policy Management Program to help ensure policies and procedures:

- Are properly communicated throughout the organization
- Are properly owned, managed and supported
- Clearly outline business objectives
- Show commitment to meet regulatory obligations
- Are focused on continual iteration and improvement
- Provide for an exception process
- Support the Policy Framework and Structure

Atlassian defines policies, standards, guidelines, and procedures and each document maintained by Atlassian is classified into one of these four categories based on the content of the document.

Item	Defines	Explanation
Policy	General rules and requirements ("state")	Outlines specific requirements or rules that must be met.
Standard	Specific details ("what")	Collection of system-specific or procedural-specific requirements that must be met by everyone.
Guideline	Common practice, recommendations and suggestions	Collection of system specific or procedural specific "suggestions" for best practice. They are not requirements to be met, but are strongly recommended. Effective policies make frequent references to standards and guidelines that exist within an organization.
Standard operating procedures	Steps to achieve Standard/Guideline requirements, in accordance with the rules ("actions")	Positioned underneath a standard or guidelines, it is a set of instructions on how to accomplish a task. From a compliance perspective, a procedure is also referred to as "Control Activity". The goal of a process/procedure is to help ensure consistent outcome defined by the Standard or Guideline.

Policy Requirements

Every policy has a Policy Owner who is responsible for managing the risk outlined in the Policy Objective. All policies are reviewed, at least annually, to help ensure they are relevant and appropriately manage risk in accordance with Atlassian's risk appetite. Changes are reviewed by the Atlassian Policy Committee (“APC”), and approved by the corresponding Policy Owner.

Policy exceptions and violations are also reviewed by the APC and actions are recommended to the Policy Owners and executive team. Policy owners can approve exceptions for a period no longer than one year.

Policy Review Process

In order to advance a policy, standard, guideline, or standard operating procedures to be publicly available internally to all Atlassian employees, each document will go through a review process. The review process follows Atlassian’s internal process where feedback is sought from a small group of knowledgeable peers on the topic. After feedback is incorporated, the draft document is submitted to the Policy Committee, either via email or via the internal corporate chat system. Any announcements of changes or updates to policies, standards or guidelines can be shared via the Blog on Policy Central.

Attachment B - Principal Service Commitments and System Requirements

Atlassian designs its processes and procedures related to the Trello system to meet its objectives for its visual collaboration tool. Those objectives are based on the service commitments that Atlassian makes to user entities, the laws and regulations that govern the provision of Trello system and the financial, operational, and compliance requirements that Atlassian has established for the system.

Security, availability and confidentiality commitments to user entities are documented and communicated in the terms of services within the sign-up page in Trello and through the Master Service Agreement ("MSA") with other vendors and enterprise customers. The description of the service offering and the system delineating the boundaries and describing relevant components is documented on the Atlassian intranet and the customer-facing website. Security, availability and confidentiality commitments are standardized and communicated to its customers via the Atlassian Trust Security Page. The security, availability and confidentiality commitments include, but are not limited to, the following:

- Operational Practices – A range of security and confidentiality controls designed to address the security and confidentiality principles of the Trello system. Such security and confidentiality controls include permitting and restricting system users to access customer data and the information they need based on their roles and responsibilities, while restricting them from accessing information not needed for their role

- Product Security – A range of security controls Atlassian implement to keep the Trello system and customer's data safe. This includes the use of encryption technologies to protect customer data in transit and at rest

- Reliability and Availability – Hosting data with Atlassian's cloud hosting partners while focusing on product resiliency to minimize downtime, as well as optimal performance with redundancy and multiple failover options within the applicable operating regions

- Security Process – A range of vulnerability and security process to detect security and vulnerability issue, which allows Atlassian to address identified gaps as soon as possible to minimize impact

Atlassian establishes operational requirements that support the achievement of security, availability and confidentiality commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Atlassian's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These 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 Trello system.