Atlassian PTY Ltd.

System and Organization Controls (SOC) 3 Report

Report on Bitbucket Cloud

Based on the Trust Services Criteria for Security, Availability, and Confidentiality

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

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

We, as management of, Atlassian are responsible for:

- Identifying the Bitbucket Cloud 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 Bitbucket Cloud System to mitigate risks that threaten the achievement of the principal service commitments and system requirement
- 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 October 31, 2019, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, and confidentiality set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Subservice Organizations Matters
Atlassian uses NTT Communications ("NTT") to provide physical safeguards and environmental safeguards. The Description (Attachment A) includes only the controls of Atlassian and excludes controls of NTT. The Description also indicates that certain trust services criteria specified therein can be met only if NTT's controls assumed in the design of Atlassian's controls are suitably designed and operating effectively along with the related controls at NTT. The Description does not extend to controls of NTT.

However, we perform annual due diligence procedures for third-party sub-service providers and based on the procedures performed, nothing has been identified that prevents us from achieving its specified service commitments.

Very truly yours,

DocuSigned by:
Erika Fisher
8A8D3A5B24B14CD...

Erika Fisher
Chief Legal Officer, Atlassian

Ernst & Young LLP
18101 Von Karman
Ave #1700
Irvine, CA 92612

Tel: +1 949 794 2300
Fax: +1 866 492 5140
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 Report of its Assertions on the Effectiveness of Its Controls over the Bitbucket Cloud Based on the Trust Services Criteria for Security, Availability, and Confidentiality (Assertion), that Atlassian Pty Ltd.'s ("Atlassian") controls over the Bitbucket Cloud (System) were effective throughout the period November 1, 2018 to October 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.

Atlassian Pty Ltd ("the Company" or "Atlassian") uses NTT Communications ("NTT") to provide physical safeguards and environmental safeguards. The Description of the boundaries of the System (Attachment A) indicates that Atlassian's controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if NTT's controls, assumed in the design of Atlassian's controls, are suitably designed and operating effectively along with related controls at the service organization. The Description presents Atlassian's system and the types of controls that the service organization assumes have been implemented, suitably designed, and operating effectively at NTT. Our examination did not extend to the services provided by NTT, and we have not evaluated whether the controls management assumes have been implemented at NTT have been implemented or whether such controls were suitably designed and operating effectively throughout the period November 1, 2018 to October 31, 2019.

Management's Responsibilities

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

- Identifying the Bitbucket Cloud 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 Bitbucket Cloud system to mitigate risks that threaten the achievement of the principal service commitments and system requirement

Building a better working world

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 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.

Building a better working world

Opinion

In our opinion, Atlassian's management's assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security, availability, and confidentiality, if the subservice organizations applied the controls assumed in the design of Atlassian's controls throughout the period November 1, 2018 to October 31, 2019.

Ernst & Young LLP

Irvine, California
January 8, 2020

Attachment A - Atlassian Service Organization's Description of the Boundaries of Its Bitbucket Cloud

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 City, 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, Statuspage, Trello, and Opsgenie.

The system in-scope for this report is primarily the Bitbucket Cloud system and supporting IT infrastructure and business processes.

Overview of Products and Service

Bitbucket Cloud is a web application that allows individuals and organizations to store and collaborate on source code using the Git or Mercurial distributed version control systems. Bitbucket is one of several products offered by Atlassian and offers seamless integration with other products offered such as Jira and Confluence. Bitbucket also offers issue tracking, asset downloads, static site hosting, a wiki, Git Large File Support, and automated build functionality. While these features and functions are available to customers, these are out of scope for the purpose of this report.

Infrastructure

Bitbucket Cloud's services and features are provided by a set of services running in the NTT data center in Ashburn, Virginia, with backup services on standby in the NTT data center in Santa Clara, California.

Separate application nodes handle web, SSH, HTTPS Git, and HTTPS Mercurial requests. A cluster of NetApp appliances provides persistent storage while PostgreSQL databases contain account and repository attributes and wiki data. Redis is used primarily as a data store for customers to gain insight on the recent activities for a given user or repository. Load balancers help ensure that incoming traffic is properly sorted by type and evenly distributed amongst application nodes. The load balancers, clusters, and Redis are out of scope for this report. Only the NetApp appliances, access to the PostgreSQL database, and backups of customer data are in scope for this report.

The processes and controls managed by the NTT data center are excluded from the scope of this report.

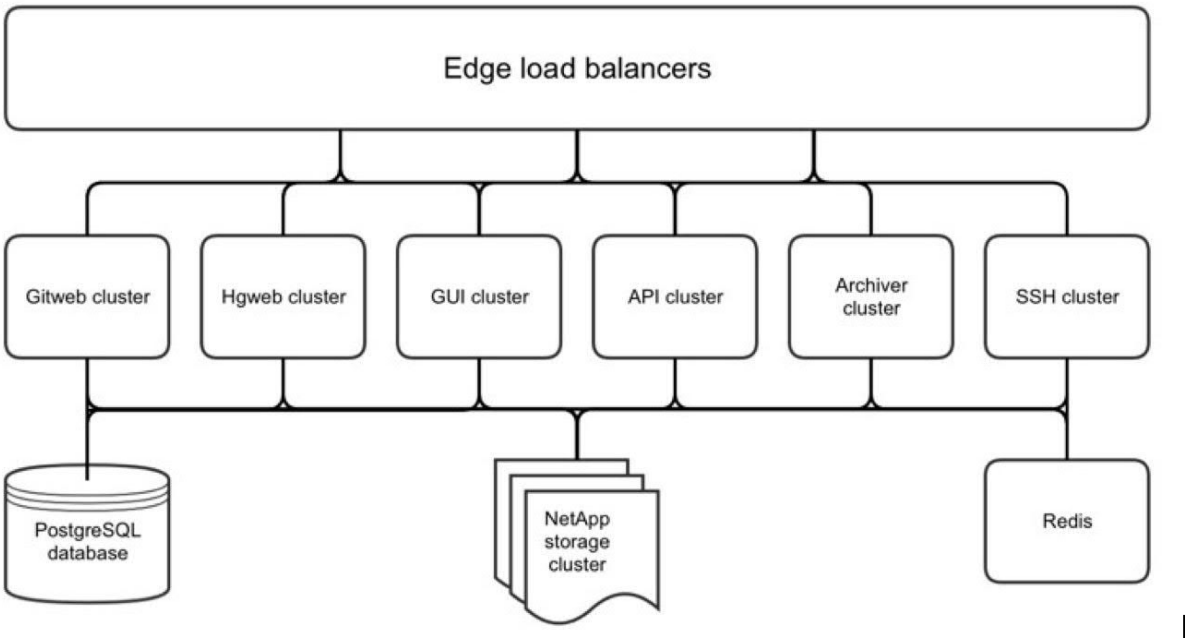

Figure 1: Architecture Diagram

Bitbucket Cloud's public network connectivity is maintained by Atlassian's Network Engineering team. Inbound packets route through Akamai, where engineers can mitigate denial-of-service attacks; outbound packets are routed through either NTT or Level 3, as appropriate for the destination.

User-initiated connections are available using IPv4 or IPv6 addresses and are available on TCP ports 22 (SSH), 80 (HTTP) or 443 (HTTPS). A special hostname, altssh.Bitbucket.org, provides SSH connectivity over port 443 for users whose networks restrict outbound connections to port 22.

All unencrypted HTTP connections are redirected to an equivalent HTTPS endpoint. Bitbucket Cloud also publishes a Strict-Transport-Security header for user agents to redirect internally to HTTPS. All inbound connections are then load-balanced, based on factors such as traffic type, host header, request path and user agent.

User requests may also be redirected to Amazon S3 for user downloads, Amazon Cloudfront for static assets in the user interface, or to a service managed by Atlassian's Media Services team for Git LFS objects or Mercurial clone bundles. These are out of scope for this report.

Bitbucket Cloud initiated connections are currently limited to notification mail to user-configured webhooks. Mail is encrypted in transit to third-party providers. Webhooks may be unencrypted at user request, or they may be sent to HTTPS servers with unverifiable certificates at user request, though both of these cases are discouraged. Both mail and webhooks originate from consistent IP addresses within Atlassian-managed space.

Within the data center, Bitbucket Cloud systems use logical binding on multiple network interfaces to provide redundancy against hardware failures. A dedicated VLAN connects application nodes to repository storage; other VLANs connect application nodes, load balancers, database servers and other resources to each other. All internal resources are isolated from the Internet by firewall.

Servers

Application nodes are stateless and clustered based on their primary service. Cluster types include, but are not limited to, the user interface; API; Git or Mercurial repository operations over SSH; Git or Mercurial repository operations over HTTP; asynchronous tasks.

Physical server configurations are managed using various tools including Puppet.

Database

Bitbucket Cloud's customer data is stored in PostgreSQL and NetApp filers (database). PostgreSQL contains account attributes, permissions, issues, pull requests and wiki data while NetApp contains customer repository data. All primary database servers reside in the physical data centers with replication nodes and backups being stored in both physical data centers as well as AWS.

Software

In-scope production servers run on CentOS servers. The following software and tools support the Bitbucket Cloud control environment:

- www.atlassian.com ("WAC") - Where customers order products, and the shopping cart is hosted
- my.atlassian.com ("MAC") - Where customers manage their current products
- Bitbucket Cloud – Atlassian's developed source code and development projects tool
- Centrify – Single sign on service used for Atlassian
- Deployment bamboo – Atlassian developed continuous integration tool used to perform automated testing and deployment activities
- Datadog – Monitoring tool
- GoogleAuth – Single sign on service used for Atlassian employees and contractors
- Jira – Ticketing system used for incident management, user access provisioning, and change management process
- Lever – Hiring tool
- NetApp – Database for customer data
- Nexpose – Vulnerability scanning tool
- Opsgenie – Atlassian's incident and alert management tool
- Pollinator – Monitoring tool
- Puppet - Open-source software configuration management tool

- StatsD - Monitoring tool
- SignalFX – Atlassian's 3rd party vendor used for system monitoring and alerting platform
- Slack – Collaboration or instant messaging tool
- Sourceclear - Software tool to identify vulnerabilities in 3rd-party libraries used by application code
- Workday – Human Resource (HR) system, including performance feedback

NTT is a third-party vendor. Atlassian performs a review of the SOC 2 report for this vendor. The evaluation of the SOC 2 report is performed and reviewed by the Risk and Compliance Team, which includes an assessment of the 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, follows up with the individual vendor. Centrify, Datadog, GoogleAuth, Lever, Nexpose, Pollinator, StatsD, SignalFX, Slack, Sourceclear, and Workday are also 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.

WAC, MAC, Jira, Bitbucket Cloud, Deployment bamboo, Jira, NetApp, Opsgenie, and Puppet are Atlassian managed tools and are in-scope in the controls discussed below.

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 sign up to Bitbucket Cloud using the website. Upon accepting the terms and conditions, and completing the sign-up flow, the customer account is created in PostgreSQL and NetApp through the use of unique identifiers. Once a repository is created in Bitbucket Cloud, it creates a specific folder in the Netapp file server (database). The path is automatically assigned by Bitbucket Cloud and creates the volume where the repository is stored and the volume contains a number of directories. The directory contains the specific repository number to which the customer is routed. Bitbucket isolates each customer's data per volume and directory in NetApp. The unique path can be seen by the customer in their Bitbucket website.

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:

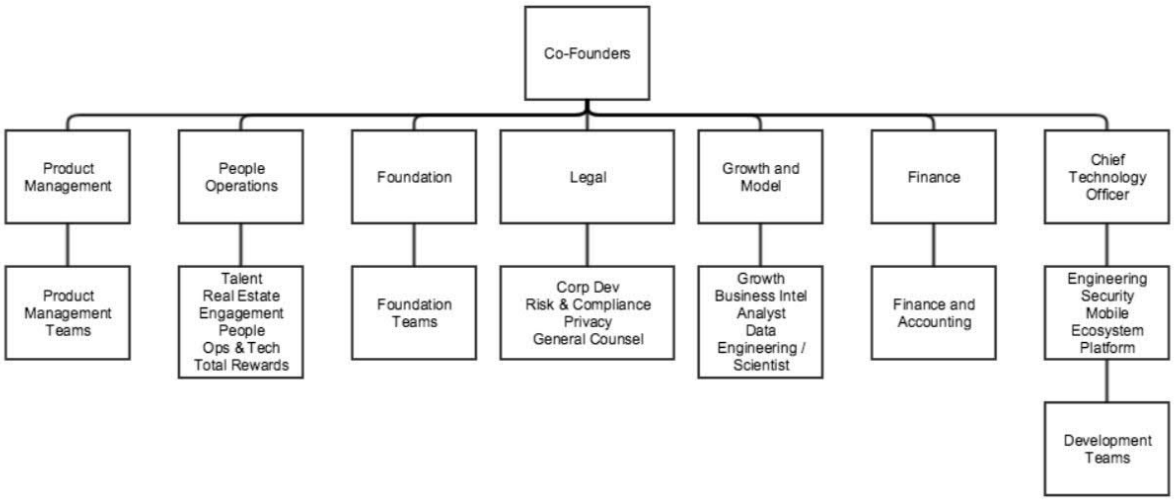

Figure 2: Atlassian's Organizational Chart

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.

Complementary Subservice Organizations Controls

Atlassian Pty Ltd ("the Company" or "Atlassian") uses NTT Communications ("NTT" or "subservice organization") to provide physical safeguards and environmental safeguards.

The affected criteria are included below along with the expected minimum controls in place at the third parties.

Criteria	Service Organization	Controls
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.	NTT	The Ashburn and Santa Clara Data Centers are remotely monitored by personnel from the Sterling and San Jose Data Centers, respectively. Data Center access is limited to authorized individuals through the use of access control cards. Additional security mechanisms are implemented, as applicable. Access to the Data Center is tracked by the system and will trigger a series of alarms if unauthorized access occurs. Customer assets, including hardware and network devices, are properly segregated from other customers using secured cabinets, cages and suites. Access to the Data Centers is granted to NTT America associates based on their job responsibilities after the Associate Enrollment Form has been approved by NTT America management. Access to the Data Centers is granted to contractors based on their job responsibilities after the appropriate contractor and NTT America approvals are documented on the Contractor Enrollment Form. Quarterly user access reviews are performed on users that have access to the Hybrid Cloud, Console Pole Server, Ops Password and NetBackup/GMP systems. Changes are made to users' access based on the review, and approval of the review is maintained in the quarterly review log. NTT America Security performs a review of data center access on at least a quarterly basis. Identified discrepancies between approval forms and access assigned are remediated.
A1.2: The entity authorizes, designs, develops or acquires, implements,	NTT	Environmental protections have been installed including the following: • Cooling systems • Battery and generator backups • Smoke detection

Criteria	Service Organization	Controls
operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.		• Dry pipe sprinklers Environmental protection equipment receive maintenance on at least an annual basis.

Management's monitoring control over sub-service providers

Due diligence procedures are in place upon engagement and at least annually for third-party service providers according to the Information Management Standard. The annual evaluation includes an assessment of the sub-service providers related SOC, ISO, Information Security Compliance Policies, response to Security & IT Questionnaire, or other attestation reports, as well as an impact analysis for any identified deficiencies.

Attachment B - Principal Service Commitments and System Requirements

Atlassian designs its processes and procedures to meet the objectives of the Bitbucket Cloud system. Those objectives are based on the service commitments that Atlassian makes to user entities, the laws and regulations that govern the provision of Bitbucket Cloud 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 Bitbucket 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 criteria of Bitbucket Cloud 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 Bitbucket Cloud 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 processes to detect security and vulnerability issues, which allow 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 Bitbucket Cloud.