Atlassian PTY Ltd.

Service Organization Controls (SOC) 3 Report

Report on Jira and Confluence Cloud

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

For the period November 1, 2017 through October 31, 2018

ATLASSIAN

Management's Assertion Regarding the Effectiveness of Its Controls Over the Jira and Confluence Cloud Based on the Trust Services Principles and Criteria for Security, Availability, and Confidentiality

We, as management of, Atlassian Pty Ltd. ("Atlassian") are responsible for designing, implementing and maintaining effective controls over the Jira and Confluence Cloud ("System") to provide reasonable assurance that the commitments and system requirements related to the operation of the System are achieved.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in Security controls, an entity may achieve reasonable, but not absolute, assurance that all security events are prevented and, for those that are not prevented, detected on a timely basis. Examples of inherent limitations in an entity's Security's controls include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer
- Ineffective controls at a vendor or business partner
- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity

Furthermore, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

We have performed an evaluation of the effectiveness of the controls over the system throughout the period November 1, 2017 to October 31, 2018, to achieve the commitments and system requirements related to the operation of the System using the criteria for the security, availability and confidentiality (Control Criteria) set forth in the AICPA's TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. Based on this evaluation, we assert that the controls were effective throughout the period November 1, 2017 to October 31, 2018 to provide reasonable assurance that:

- the System was protected against unauthorized access, use, or modification to achieve Atlassian's commitments and system requirements
- the System was available for operation and use, to achieve Atlassian's commitments and system requirements
- the System information is collected, used, disclosed, and retained to achieve Atlassian's commitments and system requirements

based on the Control Criteria.

Our attached description of the boundaries of the Jira and Confluence Cloud System identifies the aspects of the Jira and Confluence Cloud System covered by our assertion.

Very truly yours,

DocuSigned by:

D9F75B69402F4F6...

Tom Kennedy
Chief Legal Officer

Building a better
working world

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

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

Report of Independent Accountants

To the Management of Atlassian Pty Ltd.

Approach:
We have examined management's assertion that Atlassian Pty Ltd. ("Atlassian") maintained effective controls to provide reasonable assurance that:

- the Jira and Confluence Cloud System was protected against unauthorized access, use, or modification to achieve Atlassian's commitments and system requirements
- the Jira and Confluence Cloud System was available for operation and use to achieve Atlassian's commitments and system requirements
- the Jira and Confluence System information is collected, used, disclosed, and retained to achieve Atlassian's commitments and system requirements

during the period November 1, 2017 through October 31, 2018 based on the criteria for security, availability, and confidentiality in the American Institute of Certified Public Accountants' TSP section 100, *2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. This assertion is the responsibility of Atlassian's management. Our responsibility is to express an opinion 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 and appropriate 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:
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 inherent

limitations in its internal control, those controls may provide reasonable, but not absolute, assurance that its commitments and system requirements related to security, availability and confidentiality are achieved.

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. Furthermore, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion:
In our opinion, 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.

Ernst + Young LLP

San Jose, California
December 28, 2018

ATLASSIAN

Jira and Confluence Cloud Description of System
Relevant to Security, Availability, and Confidentiality

Company Overview and Background

Atlassian was founded in 2002 by Scott Farquhar and Mike Cannon-Brookes and had their Initial Public Offering ("IPO") in 2015. They have offices in San Francisco and Mountain View, California, Sydney, Australia, Manila, Philippines, Yokohama, Japan, Amsterdam, Netherlands, Austin, Texas and Bengaluru, India.

Atlassian's mission is to unleash the potential in every team. Their 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. Their products include Jira Software, Jira Service Desk, Confluence, Bitbucket, and Trello.

The systems in-scope for this report are the Jira and Confluence Cloud systems hosted at Amazon Web Services ("AWS") and the supporting IT infrastructure and business processes, excluding add-ons. This report does not include customer on-premises versions of Jira and Confluence or past Jira and Confluence hosted cloud environments.

Overview of Products and Service

Atlassian's Jira and Confluence Cloud offers several of Atlassian's products as Software as a Service: Jira Core product (Jira Service Desk as the ticketing system and Jira Software as the software), and Confluence. The Jira family of products are used to manage projects and track issues. Confluence offers document management and collaboration.

Infrastructure

Jira and Confluence Cloud are hosted at Amazon Web Services ("AWS") data centers, using the AWS infrastructure as a service offering. The various services making up the runtime and provisioning systems for Jira and Confluence Cloud are deployed in multiple AWS regions across the world (specifically us-east-1, us-west-1, us-west-2, eu-west-1, with further plans to expand to other regions).

Request flow

A typical HTTP request to the Jira or Confluence Cloud applications connect to the Cloud Smart Edge ("CSE"), which is a cluster of load balancers, closest to the user. The CSE looks up the Tenant Context Service ("TCS"), using the hostname of the request, which stores location information where the request for Jira or Confluence Cloud needs are to be routed to. It then forwards the request to the appropriate application cluster. The application, Jira or Confluence Cloud, also contacts the TCS to determine configuration information for the request, such as the database location, licensing information, etc. The application validates the login session for the user and responds to the request. If the session is not present or not valid, the user is redirected back to the original login system. During the login process, the application verifies whether the user is authorized to access the requested products. If verification passes, a valid session is created and the user is routed to the requested products. For users who are not authorized, the request is denied. Mobile applications access the Jira and Confluence Cloud APIs via the same path as the other HTTP requests.

Other flow

Other ways in which requests can be made to the application clusters is via asynchronous jobs (e.g., an application request that is not directly related to the HTTP response to the user such as sending email or running a scheduled job).

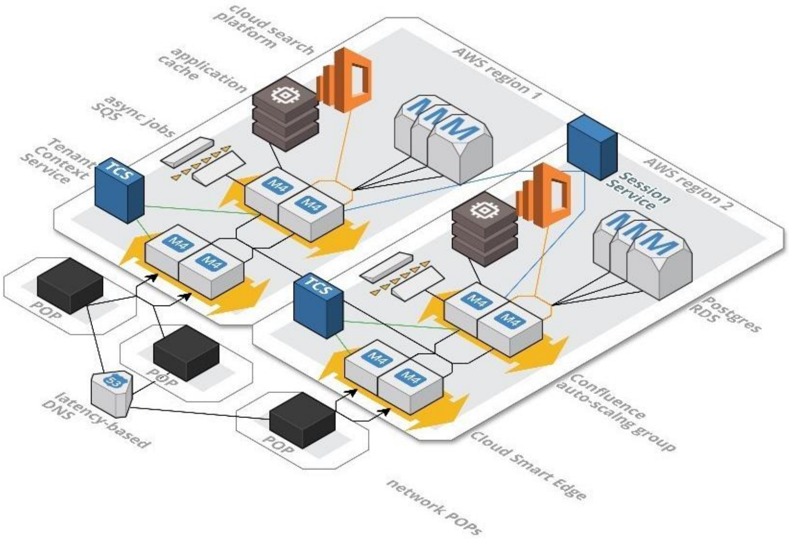

Figure 1: Confluence Architecture Diagram

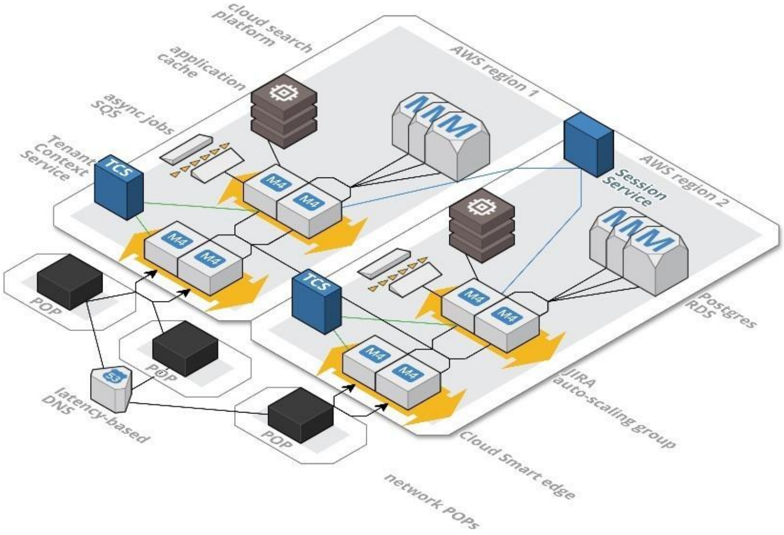

Figure 2: Jira Architecture Diagram

The difference between the Jira and Confluence Cloud architecture is the presence of the cloud search platform which is used by Confluence to provide a searchable text index into all the content.

Network

All network access to Jira and Confluence uses tenant specific DNS names, such as *tenantname*.atlassian.net (and some *tenantname*.Jira.com legacy records). At all points, the network traffic is encrypted with TLS.

All these DNS names resolve to a wildcard record under *.atlassian.net (or *.Jira.com). The DNS response is latency-based, i.e., it will return a set of IP addresses which are closest to the requestor based on latency. Atlassian has several public ingress end points, each hosted in one of Atlassian's network points of presence ("POP"). These traffic manager clusters terminate public TLS and forward the request to proxies hosted in AWS regions, closest to the data center. The proxies in AWS look up the physical location (the *shard)* for the intended tenant, based on the requested hostname, and forward the request to the correct location, which *may* be in another AWS region than the one the proxy is located in. All AWS hosted network traffic is inside Virtual Public Cloud ("VPC"), and all traffic between POPs and AWS regions, as well as between AWS regions, uses the Atlassian shared core network infrastructure, which consists of private dedicated links, which are leased from Tier-1 ISP providers.

Servers

AWS provides infrastructure as a service ("IaaS"). Jira and Confluence have separate AWS accounts for its development and production environments.

Database

Both Jira and Confluence Cloud use logically separate relational databases for each product instance, i.e., tenant data is separated at the database level. Multiple databases may share the same database server that is hosted by AWS. Each database server has an independent synchronous replica in a different availability zone within the same AWS region to mitigate the risk of data lost due to hardware failure. Database logs are kept for at least 24 hours, and backups are kept for 30 days as redundancy to allow restoration of data within a reasonable point in time, if needed.

Attachments stored in Jira or Confluence Cloud are stored in the document storage platform (Media Platform). The data in this platform is stored in Amazon S3 to increase durability guarantees, and segregated by tenant using a unique identifier that is stored in the product database. The unique identifier is stored in a DynamoDB, which relates the customer to the attachment stored in Amazon S3.

Provisioning Architecture

To provision and de-provision products for customers, Atlassian runs a set of systems, each with their own responsibility area. The customer interacts with the provisioning systems through www.atlassian.com and my.atlassian.com, where they, respectively, can purchase new products or manage their current set of products. When one of those interactions results in a product change, a request is sent to the Cloud Order Fulfilment Service ("COFS"), which manages the interaction with the billing and invoicing systems. COFS then makes a request to the Cloud Provisioning Service ("CPS"), which is responsible for running a workflow across the systems that need to provide resources for Jira and/or Confluence Cloud. The main system to be called during this workflow is Monarch, which provides a database for the product instance being provisioned. Once the provisioning workflow successfully completes, a record of all the product instance configuration is saved to the Catalogue Service. The Catalogue service then forwards copies of the record to the Tenant Context Service ("TCS"), which then makes the configuration data available to the runtime environment.

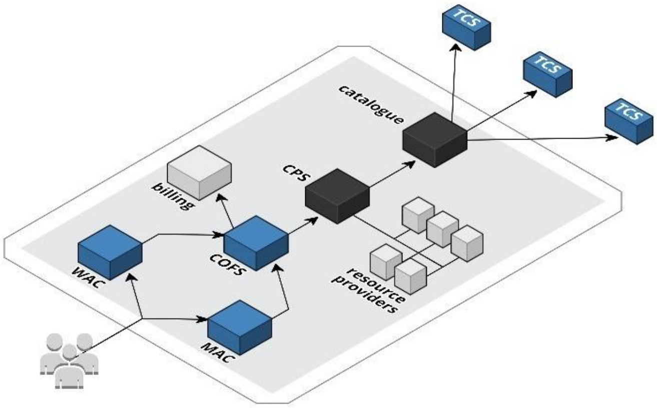

Figure 3: Provisioning Architecture

Software

The following software, services and tools support Jira and Confluence's 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
- Cloud Order Fulfilment service (COFS) - Manages the customer orders and integrates with the billing and invoicing systems
- Hosted Account Management System (HAMS) – Primary customer data process that is responsible for the core purchasing and billing functions
- Cloud Provisioning Service (CPS) - Manages the services needed to provide a product to a customer. The CPS contacts each part of the system to allocate the needed resources for a product instance, and helps ensure that all these resource allocations complete correctly and in the right order.
- Catalogue Service and Catalogue Data Search Service (CS and CDSS) - Administrative store for the configuration of a product and customer
- Tenant Catalogue Service (TCS) - Stores the product-specific configuration for a customer for consumption at runtime

- Monarch (database manager) - Manages the per-customer databases for the products, using AWS RDS
- Cloud Search Platform (CSP) - The search engine for Confluence Cloud (based on Elastic Search)
- Media Services (document store) - Stores attachments for Jira and Confluence Cloud
- Identity services - Management of users, authentication and authorization
- Auth0 – Identity and access management software
- Centrify – Single sign on service used for Atlassian
- Jira - Ticketing system used for incident management, user access provisioning, and change management process
- Confluence - System used for documentation about process and services
- Bamboo - Bamboo is Atlassian’s developed continuous integration tool used to perform automated testing and deployment activities
- Bitbucket Server - Atlassian’s developed source code and development projects tool
- AWS Glacier - data archiving and long-term backup storage service
- Workday – Human Resources (HR) system
- Impraise – Performance feedback tool
- SmartRecruiters - Hiring tool (used between the period from November 1, 2017 to June 30, 2018)
- Lever – Hiring tool (effective as of July 1, 2018)
- AWS Cloudwatch – Monitoring of availability tool
- Datadog – Monitoring of security and availability tool and job schedules in Atlassian
- Pollinator – Monitoring of security and availability tool
- PagerDuty – Alerting tool for monitoring of availability
- Stride – Messaging tool for alerting on availability
- Alfred – Monitoring of access tool (AWS account management tool managed by Atlassian)

AWS is managed by a third-party vendor. Atlassian performs a review of the SOC2 reports as discussed below. The evaluation of the SOC report is performed and reviewed by the Risk and Compliance Team, which includes an assessment of the complimentary user entity control, subservice organizations, and mapping of the controls to key IT risks. If there are exceptions, Atlassian will review the severity and impact of the exceptions, and if needed, follow up with the individual vendor. Datadog, Pollinator, Centrify, Workday, Auth0, Impraise, Lever, and SmartRecruiters are managed by third party vendors, however, customer data is not stored in these applications. These are supporting and monitoring tools not in scope for the SOC3 report 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, vendors are required to sign the vendor agreements.

Data

Customers sign up for Jira and/or Confluence Cloud on www.atlassian.com. Upon sign-up, dedicated product databases are created in the AWS Postgres RDS clusters, which are logically separated from other customers' data, using both a separate database and separate credentials. Once complete, the customer can start using Jira and/or Confluence Cloud. Metadata information about the customer is also written into the Catalogue Service ("CS") database which stores the master copy of the customers' configuration. The identity details of the site administrator and any users they create are kept in a dedicated Atlassian identity platform, which manages the storage and security of this data, and which provides interfaces for login, authentication, authorization, and session management. For performance reasons, user information is synchronized to the product databases. Production customer data is encrypted in transit and is managed by AWS. AWS' SOC2 report is reviewed at least annually by Atlassian. Customer data is not encrypted at rest, however, customer attachments in Jira and Confluence are encrypted in the Media Platform. 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:

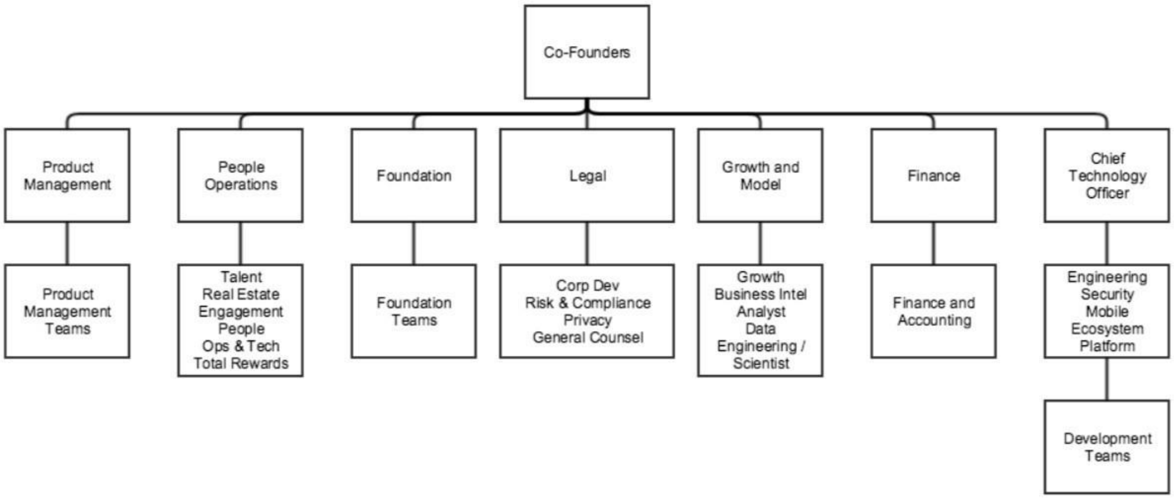

Figure 4: Atlassian's Organizational Chart

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.