Atlassian PTY Ltd.

System and Organization Controls (SOC) 3 Report

Report on Halp

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

For the period January 1, 2020 through October 31, 2020

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

We, as management of, Atlassian are responsible for:

- Identifying the Halp (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 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 January 1, 2020 to October 31, 2020 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 Amazon Web Services ("AWS") and MongoDB to provide physical safeguards, environmental safeguards, infrastructure support and management, and storage services. Atlassian uses Heroku to provide infrastructure support and management, and storage services. The System (Attachment A) includes only the controls of Atlassian and excludes controls of the AWS, Heroku, and MongoDB. The Description also indicates that certain trust services criteria specified therein can be met only if AWS's, MongoDB's and Heroku's controls assumed in the design of Atlassian's controls are suitably designed and operating effectively along with the related controls at the Service Organizations. The Description does not extend to controls of AWS, MongoDB, and Heroku.

However, we performed 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:
Stan Shepard
B2[illegible]FC...

Stan Shepard
Deputy General Counsel, Atlassian

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

Tel: +1 949 794 2300
Fax: +1 866 492 5140
ey.com

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 Halp System Based on the Trust Services Criteria for Security, Availability, and Confidentiality (Assertion), that Atlassian's controls over the Halp System (System) were effective throughout the period January 1, 2020 to October 31, 2020, 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 Amazon Web Services ("AWS") and MongoDB to provide physical safeguards, environmental safeguards, infrastructure support and management, and storage services and Heroku to provide infrastructure support and management, and storage services. 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 AWS, MongoDB, and Heroku controls, assumed in the design of Atlassian's controls, are suitably designed and operating effectively along with related controls at the service organizations. The System presents Atlassian's system and the types of controls that the service organization assumes have been implemented, suitably designed, and operating effectively at AWS, MongoDB, and Heroku. Our examination did not extend to the services provided by AWS, MongoDB and Heroku, and we have not evaluated whether the controls management assumes have been implemented at AWS, MongoDB, and Heroku have been implemented or whether such controls were suitably designed and operating effectively throughout the period January 1, 2020 to October 31, 2020.

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 Halp System (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 System to mitigate risks that threaten the achievement of the principal service commitments and system requirement

Building a better working world

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

Tel: +1 949 794 2300
Fax: +1 866 492 5140
ey.com

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.

Opinion

In our opinion, Atlassian's management assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security, availability, and confidentiality (applicable trust services criteria), and if the subservice organizations applied the controls assumed in the design of Atlassian's controls throughout the period January 1, 2020 to October 31, 2020.

Ernst & Young LLP

December 22, 2020
Irvine, California

Attachment A – Atlassian Service Organization's Description of the Boundaries of Halp

Company Overview and Background

Halp was founded in 2017 and was acquired by Atlassian in May 2020. Atlassian was founded in 2002 by Scott Farquhar and Mike Cannon-Brookes. Atlassian had its Initial Public Offering ("IPO") in 2015.

Atlassian has offices across the globe including the United States (San Francisco, Mountain View, New York City, Austin, Boston), Australia (Sydney), Philippines (Manila), Japan (Yokohama), Netherlands (Amsterdam), Turkey (Ankara), and India (Bengaluru).

Atlassian's mission is to unleash the potential in every team. Its collaboration software helps teams organize, discuss, and complete shared work. Thousands of teams across large and small organizations worldwide 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, Jira Service Management, Confluence, Bitbucket, Statuspage, Trello, Opsgenie, Jira Align, and Halp.

The systems in-scope for this report is the Halp system hosted at Amazon Web Services ("AWS") and the supporting IT infrastructure and business processes, excluding add-ons.

Overview of Products and Service

Halp is a conversational ticketing solution for modern IT and Operations teams to assign, prioritize, manage, and report on requests from various platforms.

The Halp application enables the following tasks related to internal ticketing:

- Creating tickets in platforms anywhere end users prefer (email, slack, web, etc.)
- Triaging and collaborating on tickets in a conversational manner
- Providing scope-based permissions and the ability to collaborate privately
- Setting custom fields and statuses on tickets
- Setting custom working hours and service-level agreements (SLAs) for tickets
- Managing agent roles and permissions
- Routing tickets to the appropriate group of people
- Providing reports and CSV exports on ticket data
- Providing reporting in a variety of formats
- Automating workflows with Halp's Recipe Engine
- Communicating changes to tickets across multiple platforms (email, slack, web, etc.)
- Integrating with other ticketing systems with a two-way sync functionality
- Automating a subset of ticket resolutions

- Adding followers to tickets across platforms

When a ticket is created in Halp, it opens two conversations: one for the requester and one for the agent. The agent's conversation is routed to the appropriate team based on a set of user configurable conditions. For example, if an end user has an IT related request, Halp will automatically route the request to the IT team. From there, the IT team can assign, edit, collaborate, and escalate the ticket.

Infrastructure

Halp is 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 Halp are deployed in AWS us-east-1. Prior to acquisition, the Halp application was hosted in Heroku.

Halp's primary database is MongoDB which is hosted on AWS us-east-1 with failover in us-west-2.

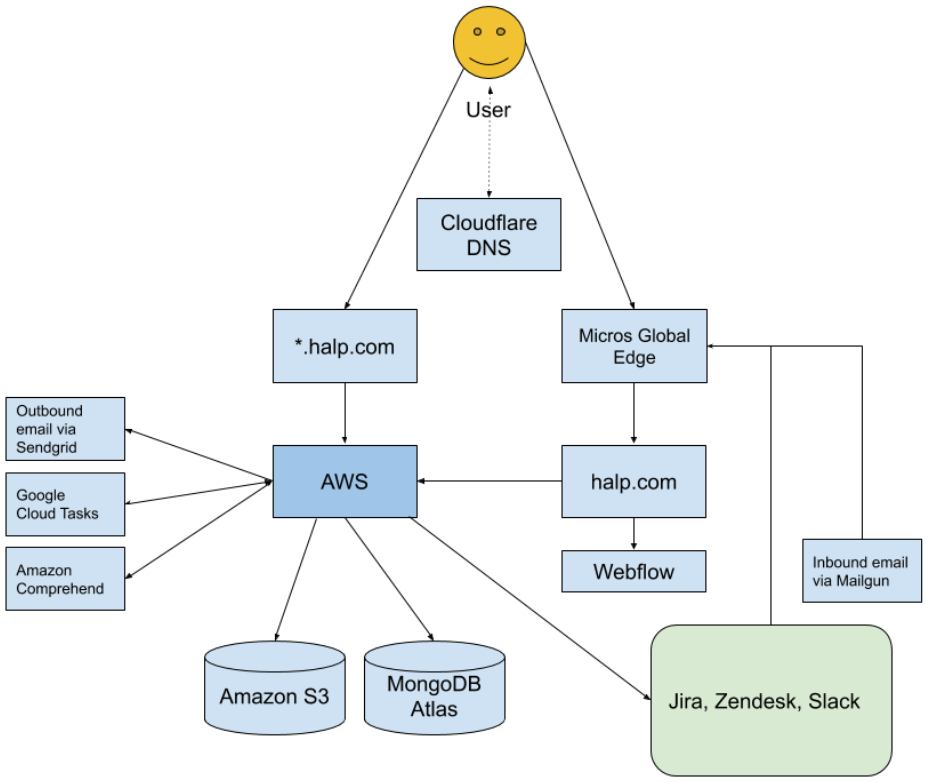

Figure 1: Halp's Architecture Diagram

Servers

AWS provides Infrastructure-as-a-Service ("IaaS") and the initial creation of the virtual servers which run Halp. However, the software and operating system configurations are managed by Atlassian. The AWS infrastructure spans multiple data centers and regions and Halp has separate AWS accounts for its development and production environments.

Database

Halp uses 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 and managed by MongoDB. The primary database server has two replicas, and the failover database server has a single replica.

Each database server has an independent synchronous replica in a different availability zone within the same AWS region to mitigate the risk of data loss due to hardware failure.

Attachments stored on Halp tickets are stored in the document storage platform. The data in this platform is stored in Amazon S3 to increase durability and segregate by tenant using a unique identifier.

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

Software

The following software, services and tools support the control environment of Halp:

Component	Description
Hosting Systems	• Heroku (*1/1/2020 to 5/30/2020*) • Amazon EC2
Storage and Database	• MongoDB • Amazon Simple Storage Service (S3)
Network	• Amazon Virtual Private Cloud • Amazon Load Balancers • Corporate firewall • Cloudflare
Build, Release, and Continuous Integration Systems	• Github (*1/1/2020 to 6/30/2020*) • Bitbucket (*7/1/2020 to 10/31/2020*)
Access Management	• Active Directory • Idaptive (Single Sign On) • Duo (Two-factor authentication) • 1Password • Retool
Monitoring and Alerting	• Splunk • SignalFX • Opsgenie • Scalyr • Vanta
Platforms	• Slack
Vulnerability Scanning	• Github *(1/1/2020 to 6/30/2020)* • SourceClear *(7/1/2020 to 10/31/2020)* • Cloud Conformity *(7/1/2020 to 10/31/2020)*
Human Resource	• JustWorks HR *(1/1/2020 to 5/30/2020)* • Workday *(6/1/2020 to 10/31/2020)* • Lever *(6/1/2020 to 10/31/2020)*

AWS, MongoDB, and Heroku is a third-party vendor that provides physical safeguards, environmental safeguards, infrastructure support and management, and storage services. Atlassian has identified the complementary subservice organization controls of AWS, MongoDB, and Heroku to achieve the applicable trust services criteria. The other third-party vendors mentioned above are only applicable to support certain controls and criteria.

Data

Customers sign up for Halp on https://www.halp.com. Upon accepting the terms and conditions, and completing the sign-up process, a new database record and unique identifier is created in MongoDB for that customer account and their organization. The unique ID is used thereafter for associating data with the specific organization. The data is logically separated from other users' and organizations' data using these unique ID's. All user created data are similarly assigned unique identifiers such that they can be correctly associated to users and organizations. Static assets and attachments that users upload to customize their content are uploaded to AWS S3 and are linked via unique identifiers within the database.

Customer data is encrypted at rest and external connections to Halp are encrypted in transit via the TLS protocol. Customer data is only stored in production environments and is not transferred to any non-production environment.

Organizational Structure

Pre-Acquisition

Halp had a staff of approximately 14 employees organized in the following functional areas:

- Engineering: Software engineers, product designers, and any other technical staff devoted to the production and maintenance of Halp systems and applications.
- Executive: The executives and founders of Halp. These individuals are responsible for setting the vision and strategy of the company, as well as implementing and maintaining the security policies and culture at Halp.
- Operations: Operations staff, including HR, IT, office administration, legal, accounting, and finance. The operations staff are responsible for functions like onboarding, background checks, endpoint setup, physical security, and enforcement of security policies.
- Marketing: Marketing staff are responsible for communicating Halp's value to the rest of the world.
- Sales: Sales staff are responsible for negotiating contracts and deals.

Post-Acquisition

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:

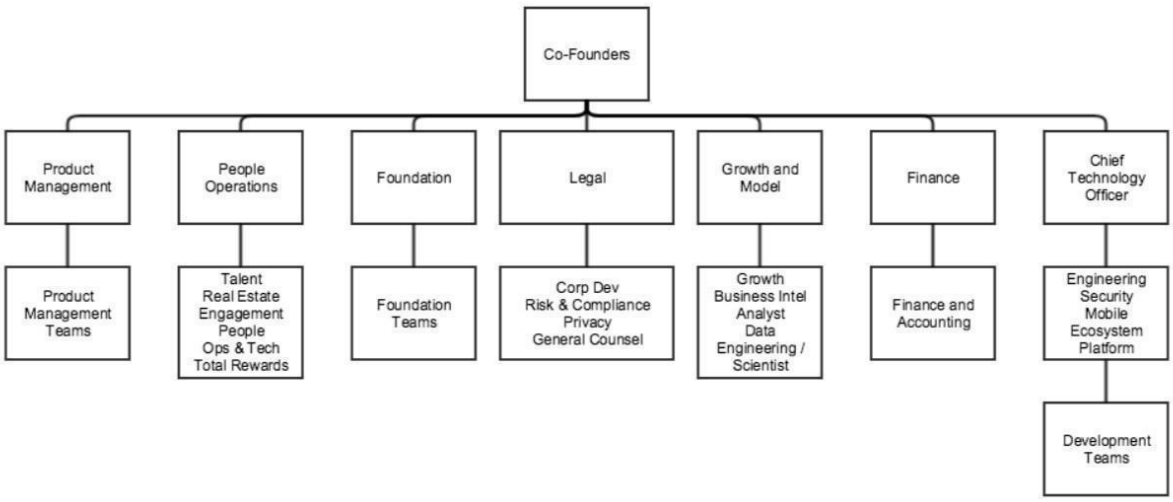

Figure 2: Atlassian's Organizational Chart

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 are 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 maintain 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 hold 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 utilizes subservice organizations to perform certain functions as described in the description above. Rather than duplicate the control tests, controls at Amazon Web Services, MongoDB, and Heroku are not included in the scope of this report. The affected criteria are included below along with the expected controls of Amazon Web Services ("AWS"), MongoDB, and Heroku.

Criteria	Service Organization	Controls
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.	AWS, MongoDB, Heroku	IT access above least privileged, including administrator access, is approved by appropriate personnel prior to access provisioning. IT access privileges are reviewed on a quarterly basis by appropriate personnel. User access to systems is revoked timely upon termination. Data is encrypted in transit in AWS.
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.	AWS, MongoDB, Heroku	Physical access to the computer rooms, which house the entity's IT resources, servers, and related hardware, is restricted to authorized individuals through a badge access system or equivalent, and monitored by video surveillance. Requests for physical access privileges require management approval. Documented procedures exist for the identification and escalation of potential physical security breaches. Visitors must be signed in by an authorized workforce member before gaining entry and must be escorted at all times.
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.	AWS, MongoDB, Heroku	Changes are authorized, tested, and approved prior to implementation.

Criteria	Service Organization	Controls
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.	AWS, MongoDB, Heroku	Environmental protections have been installed including the following: • Cooling systems • Battery and generator backups • Smoke detection • Dry pipe sprinklers Environmental protection equipment receive maintenance on at least an annual basis.

Management's Monitoring Control over the Subservice 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 related to the Halp system. Those objectives are based on the service commitments that Atlassian makes to user entities, the laws and regulations that govern the provision of Halp 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 Halp 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 the Halp 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 implements to keep the Halp system and customer's data safe. This includes the use of encryption technologies to protect customer data at rest and in transit, and formal processes to grant and revoke access to customer data.
- 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 failover options globally while maintaining multiple locations and availability zones across AWS regions.
- Security Process – A range of vulnerability and security processes to detect security and vulnerability issues, 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 Halp system.