Report on Atlassian Corporation Plc's Description of Its Halp System and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security, Availability, and Confidentiality Throughout the Period October 1, 2021 to September 30, 2022

SOC 2® - SOC for Service Organizations: Trust Services Criteria

Table of Contents

Section 1

Independent Service Auditor’s Report

Independent Service Auditor's Report

To: Atlassian Corporation Plc ("Atlassian")

Scope

We have examined Atlassian's accompanying description in Section 3 titled "Atlassian Corporation Plc's Description of Its Halp System Throughout the Period October 1, 2021 to September 30, 2022" (description) based on the criteria for a description of a service organization's system set forth in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that Atlassian's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Atlassian, to achieve Atlassian's service commitments and system requirements based on the applicable trust services criteria. The description presents Atlassian's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Atlassian's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Atlassian uses subservice organizations to provide data center colocation services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Atlassian, to achieve Atlassian's service commitments and system requirements based on the applicable trust services criteria. The description presents Atlassian's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Atlassian's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The information included in Section 5, "Other Information Provided by Atlassian Corporation Plc That Is Not Covered by the Service Auditor's Report," is presented by Atlassian's management to provide additional information and is not a part of Atlassian's description of its Halp System made available to user entities during the period October 1, 2021 to September 30, 2022. The information included in Atlassian's responses to testing exceptions has not been subjected to the procedures applied in the examination and, accordingly, we express no opinion on it.

Service Organization's Responsibilities

Atlassian is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Atlassian's service commitments and system requirements were achieved. In Section 2, Atlassian has provided the accompanying assertion titled "Assertion of Atlassian Corporation Plc Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated

therein. Atlassian is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description 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, in all material respects, the description is presented in accordance with the description criteria and whether the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves—

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also,

the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in Section 4, “Trust Services Criteria, Related Controls, and Tests of Controls Relevant to the Security, Availability, and Confidentiality Categories” of this report.

Opinion

In our opinion, in all material respects—

a. The description presents Atlassian’s Halp System that was designed and implemented throughout the period October 1, 2021 to September 30, 2022, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that Atlassian’s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Atlassian’s controls throughout that period.

c. The controls stated in the description operated effectively throughout the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that Atlassian’s service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of Atlassian’s controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Atlassian, user entities of Atlassian’s Halp System during some or all of the period October 1, 2021 to September 30, 2022, business partners of Atlassian subject to risks arising from interactions with Atlassian’s Halp System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.

- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties. If a report recipient is not a specified party as defined above and has obtained this report, or has access to it, use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against Coalfire Controls, LLC as a result of such access. Further, Coalfire Controls, LLC does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Coalfire Controls LLC

Westminster, Colorado
December 8, 2022

Section 2

Assertion of Atlassian Corporation Plc Management

Assertion of Atlassian Corporation Plc ("Atlassian") Management

We have prepared the accompanying description in Section 3 titled "Atlassian Corporation Plc's Description of Its Halp System Throughout the Period October 1, 2021 to September 30, 2022" (description), based on the criteria for a description of a service organization's system set forth in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the Halp System that may be useful when assessing the risks arising from interactions with Atlassian's system, particularly information about system controls that Atlassian has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Atlassian, to achieve Atlassian's service commitments and system requirements based on the applicable trust services criteria. The description presents Atlassian's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Atlassian's controls.

Atlassian uses subservice organizations for data center colocation services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Atlassian, to achieve Atlassian's service commitments and system requirements based on the applicable trust services criteria. The description presents Atlassian's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Atlassian's controls. The description does not disclose the actual controls at the subservice organizations.

We confirm, to the best of our knowledge and belief, that:

a. The description presents Atlassian's Halp System that was designed and implemented throughout the period October 1, 2021 to September 30, 2022, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that Atlassian's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Atlassian's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that Atlassian's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of Atlassian's controls operated effectively throughout that period.

Adrian Ludwig
Chief Trust Officer
Atlassian Corporation Plc

Section 3

Atlassian Corporation Plc's Description of Its Halp System Throughout the Period October 1, 2021 to September 30, 2022

Type of Services Provided

Company Overview and Background

Halp was founded in 2017 and was acquired by Atlassian ("the Company") 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 in the United States (San Francisco, Mountain View, New York City, Austin, Boston), Australia (Sydney), the Philippines (Manila), Japan (Yokohama), the Netherlands (Amsterdam), Poland (Gdansk), Turkey (Ankara), and India (Bengaluru). Additionally, Atlassian embraces distributed teamwork, enabling employees to work remotely across Australia, Canada, France, Germany, India, Japan, New Zealand, the Netherlands, the Philippines, the United Kingdom, the United States, and Turkey.

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 Suite (Software and Jira Work Management), Jira Service Management, Jira Product Discovery, Confluence, Atlas, Atlassian Analytics, Bitbucket Cloud, Compass, Data Lake, Forge, Insight, Statuspage, Trello, Opsgenie, Jira Align, and Halp. Refer to the "Overview of Products and Services" section below for the systems in-scope for this report.

The systems in scope for this report are the Halp system ("Halp") and the related MongoDB databases, which are hosted on Amazon Web Services (AWS), and the supporting information technology (IT) infrastructure and business processes, excluding add-ons. This report does not include on-premises versions (e.g., Jira and Confluence Server and Data Center), add-ons from the Marketplace, or open-source downloadables added by customers to their instances.

Overview of Products and Services

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 from platforms anywhere end users prefer (e.g., email, Slack, web)
- 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 (e.g., email, Slack, web)

- 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.

Principal Service Commitments and System Requirements

Atlassian designs its processes and procedures to meet the objectives of 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 the 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 the Atlassian Trust Security Page. 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. The security, availability, and confidentiality commitments include, but are not limited to, the following:

Trust Services Category	Service Commitments
Security	Atlassian will develop and maintain technical and organizational measures designed to protect customer information.
Availability	Atlassian will use commercially reasonable efforts to maintain the availability of the system.
Confidentiality	Atlassian will not use or disclose confidential information to any third party unless they have a business need to know.

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.

- 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 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. Optimal performance with global redundancy and failover options including maintaining multiple locations and availability zones (AZs) 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.

The Components of the System Used to Provide the Services

The boundaries of Halp are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of Halp.

The components that directly support the services provided to customers are described in the subsections below.

Infrastructure

Halp is hosted at 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.

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

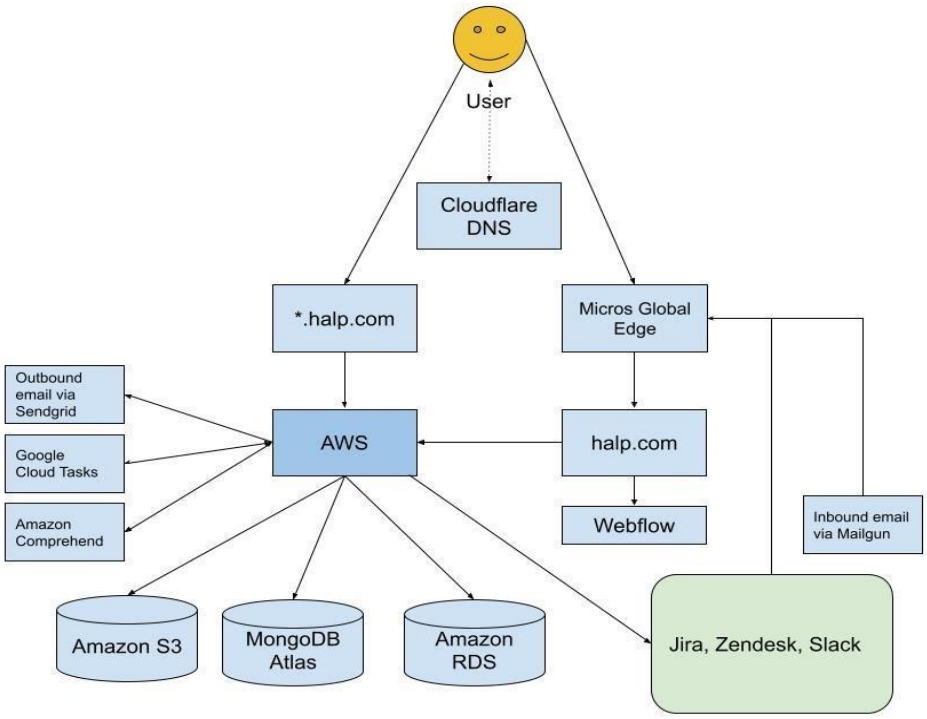

Figure 1: Halp's Architecture Diagram

Servers

AWS provides infrastructure-as-a-service (IaaS) and the initial creation of the virtual servers that 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). MongoDB is the primary database server that stores customer information and has two replicas, and the failover database server (Amazon Relational Database Service [Amazon RDS]) has a single replica.

Each database server has an independent synchronous replica in a different AZ 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 in Amazon Simple Storage Service (Amazon S3). The data in this platform is stored to increase durability and segregate by tenant using a unique identifier.

All production customer data is encrypted at rest and external connections to Halp are encrypted in transit via the Transport Layer Security (TLS) 1.2 protocol.

Software

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

Software	
Component	**Description**
Hosting Systems	• Amazon Elastic Compute Cloud (Amazon EC2)
Storage and Database	• Amazon RDS • Amazon S3 • MongoDB
Network	• Amazon Virtual Private Cloud (Amazon VPC) • Amazon load balancers • Cloudflare • Corporate firewall
Build, Release, and Continuous Integration Systems	• Bitbucket • Bitbucket Pipelines • Deployment Bamboo
Access Management	• Active Directory • Idaptive (single sign-on [SSO]) • Duo (two-factor authentication) • 1Password • Retool (end of life was on April 1, 2022)

Software	
Component	**Description**
Monitoring and Alerting	• Splunk • SignalFX • Opsgenie • Sentry
Vulnerability Scanning	• Cloud Conformity • Nexpose • Snyk • SourceClear
Human Resources (HR)	• Workday • Lever

AWS is responsible for providing physical safeguards, environmental safeguards, infrastructure support and management, and storage services, and MongoDB, which provides database services, are third-party vendors. Atlassian has identified the complementary subservice organization controls of AWS and MongoDB to achieve the applicable trust services criteria which are listed in the Subservice Organizations and Complementary Subservice Organization Controls section of this report. The other third-party vendors mentioned above are only applicable to support certain controls and criteria which are the responsibility of Atlassian.

People

The Company develops, manages, and secures Halp via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
Co-Founders and Executive Management	Responsible for overseeing company-wide activities, establishing and accomplishing goals, and managing objectives.
Engineering	Responsible for the development, testing, deployment, and maintenance of new code for Halp.
Trust	Responsible for managing access controls and the security of the production environment.
Product Management	Responsible for overseeing the product life cycle, including adding new product functionality.
People (in partnership with the people leaders)	Focuses on determining the right talent strategy to deliver against the needs of Atlassian. The People team is responsible for talent acquisition and learning, total rewards and technology, and workplace experiences.
Platform and Enterprise Cloud	Focuses on validating the demands of customers and provides insight and guidance around minimum viable product and user experience.

People	
Group/Role Name	**Function**
Foundation	Exists to harness the resources of Atlassian to champion organizations who believe that education is the key to eliminating 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, and public relations.
Finance	Responsible for handling finance and accounting.
Chief Technology Officer (Technology Operations)	Oversees Engineering, Trust, Risk and Compliance, Information Security, Mobile, Ecosystem, and Platform.

The following organization chart reflects the Company's internal structure related to the groups discussed above:

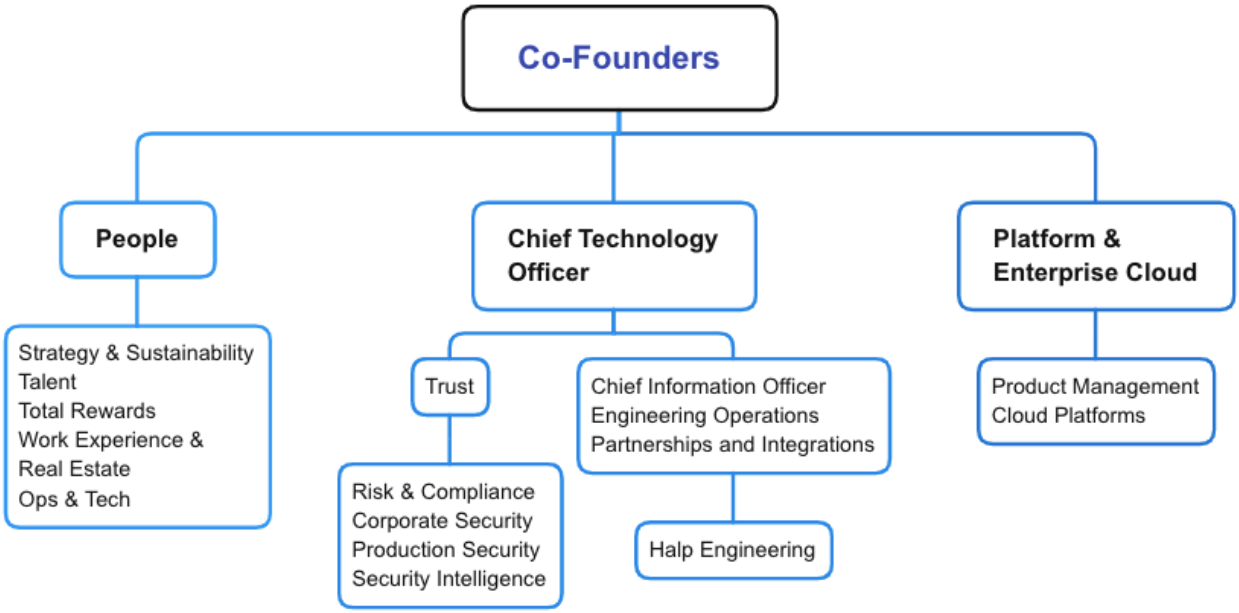

Figure 2: Halp Organization Chart

Policies and Procedures

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

- Properly communicated throughout the organization
- Properly owned, managed, and supported
- Clearly outlining business objectives
- Showing commitment to meet regulatory obligations
- Focused on continual iteration and improvement
- Provided for an exception process
- Supported by 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.

The following table details the procedures as they relate to the operation of Halp:

Policies, Standards, Guidelines, and Procedures		
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 practices. 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 guideline, a standard operating procedure is a set of instructions on how to accomplish a task. From a compliance perspective, a procedure is also referred to as a control activity. The goal of a process/procedure is to help achieve a 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

To advance a policy, standard, guideline, or standard operating procedure 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 updates to policies, standards, or guidelines are shared via email and the internal website where all policies are stored.

Data

Customers sign up for Halp on https://www.halp.com. Once a customer accepts the terms and conditions and completes 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 IDs. All user-created data is similarly assigned unique identifiers such that those identifiers can be correctly associated with users and organizations. Static assets and attachments that users upload to customize their content are uploaded to Amazon S3 and are linked via unique identifiers within the database.

Encryption is enabled for data at rest, and external connections to Halp are encrypted in transit via the TLS 1.2 protocol. Customer data is only stored in production environments and is not transferred to any non-production environment.

System Incidents

There were no identified significant system incidents that (a) were the result of controls that were not suitably designed or operating effectively to achieve one or more of the service commitments and system requirements or (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements from October 1, 2021 to September 30, 2022.

The Applicable Trust Services Criteria and Related Controls

Applicable Trust Services Criteria

The Trust Services Categories that are in scope for the purposes of this report are as follows:

- *Security:* Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability or confidentiality of information or systems and affect the entity's ability to meet its objectives.
- *Availability:* Information and systems are available for operation and use to meet the entity's objectives.
- *Confidentiality:* Information designated as confidential is protected to meet the entity's objectives.

Many of the criteria used to evaluate a system are shared amongst all in-scope categories; for example, the criteria related to risk assessment apply to the security, availability, and confidentiality categories. As a result, the criteria for the security, availability and confidentiality categories are organized into (a) the criteria that are applicable to all categories (common criteria) and (b) criteria applicable only to a single category. The common criteria constitute the complete set of criteria for the security category. For the categories of availability, and confidentiality, a complete set of criteria is comprised of all the common criteria and all the criteria applicable to the category being reported on.

The common criteria are organized as follows:

1. *Control environment:* The criteria relevant to how the entity is structured and the processes the entity has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values, qualifications of personnel, and the environment in which they function.
2. *Communication and information:* The criteria relevant to how the entity communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.
3. *Risk assessment:* The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.
4. *Monitoring activities:* The criteria relevant to how the entity monitors the system, including the suitability and design, and operating effectiveness of the controls, and acts to address deficiencies identified.
5. *Control activities:* The criteria relevant to the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out.
6. *Logical and physical access controls:* The criteria relevant to how the entity restricts logical and physical access, provides and removes that access, and prevents unauthorized access.
7. *System operations:* The criteria relevant to how the entity manages the operation of system(s) and detects and mitigates processing deviations, including logical and physical security deviations.
8. *Change management:* The criteria relevant to how the entity identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
9. *Risk mitigation:* The criteria relevant to how the entity identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

This report is focused solely on the security, availability, and confidentiality categories. The Company has elected to exclude the processing integrity and privacy categories.

Control Environment

The objective of Atlassian's control environment is to set the tone for the organization's internal control.

Integrity, Ethical Values, and Competence

Integrity, ethical values, and competence are key elements of Atlassian's control environment. Atlassian employees are required to acknowledge the Code of Conduct. The HR Operations team is involved in reviewing and monitoring that these policies and agreements are acknowledged, and background screening is followed through in a timely manner.

Employees and contractors with access to Atlassian systems are asked to re-acknowledge the Code of Conduct annually.

Learning and Development

Atlassian requires its employees to complete anti-harassment training and offers opportunities for technical training and professional development. Regarding technical training and professional development, Atlassian believes every employee could reach their fullest potential and do the best work of their lives with the right support. Autonomy, mastery, and purpose are cornerstones of this philosophy. Therefore, Atlassian lowers the barriers of entry for new learning, making it possible for employees to take charge of their learning needs and own more of their growth and development. Atlassian offers professional development for employees via training or tuition reimbursements and online learning management systems.

Learning Central is Atlassian's primary learning and development hub to help employees pursue new ways to learn and grow. Everything from custom growth plan templates to online resources and other learning experiences are available through Learning Central. The learning hub provides growth support for all levels of employees at Atlassian.

- Growth Plans were created to help employees understand expected attitudes, behavior, and skills that contribute to success in a role and connect them to resources aimed at improving those skills. The Learning and Development team has done research to map formalized competencies to most roles at Atlassian, particularly those that are customer and product facing. Managers and employees use these competencies to see what is required for success in a position and what areas an employee needs further development/training around. Based on these gaps, managers and the Learning and Development team can recommend training, self-study, or coaching as needed.
- Degreed, Get Abstract, LinkedIn Learning, Learndot, and Intellum are third-party tools Atlassian uses to enable employees to access thousands of online learning resources for free. They also serve as the primary portals to host internally created learning paths that guide employees through targeted learning experiences, whether they are new hires, new managers, or seasoned employees taking their first steps into people leadership.

Board of Directors, Audit Committee, and Assignment of Authority and Responsibility

Atlassian’s Board of Directors and various subcommittees (including Audit, Nominating and Governance, Compensation, and Leadership Development) meet at least annually to review committee charters and corporate governance, which defines their roles, responsibilities, member qualifications, meeting frequency, and other discussion topics. Meeting minutes of the annual meetings are recorded, including participants and the date the meeting occurred. The process of identifying and reviewing Board of Directors candidates is defined in the Nominating and Governance Committee charter.

The executive team sets strategic operational objectives at least annually during Values, Targets, Focus, and Metrics (VTFM) sessions. Each target is communicated down into each of the product groups for execution by the Management team. Progress toward targets is evaluated at least quarterly by the Executive and Management teams.

The audit committee charter is published on Atlassian’s investors website under Governance Documents. The audit committee charter includes the roles, responsibilities, key activities, and meetings. Qualifications for the audit committee’s financial expert are also outlined and defined within the audit committee charter. The audit committee meeting calendar and meeting agenda are developed. The audit committee meeting minutes are published annually as well. The results of the audit committee meeting results are published after the meeting has been completed. The agenda includes items to be discussed, as well as general

questions and answers about the annual general meeting, such as who is allowed to vote at the annual general meeting.

Organizational Structure

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

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

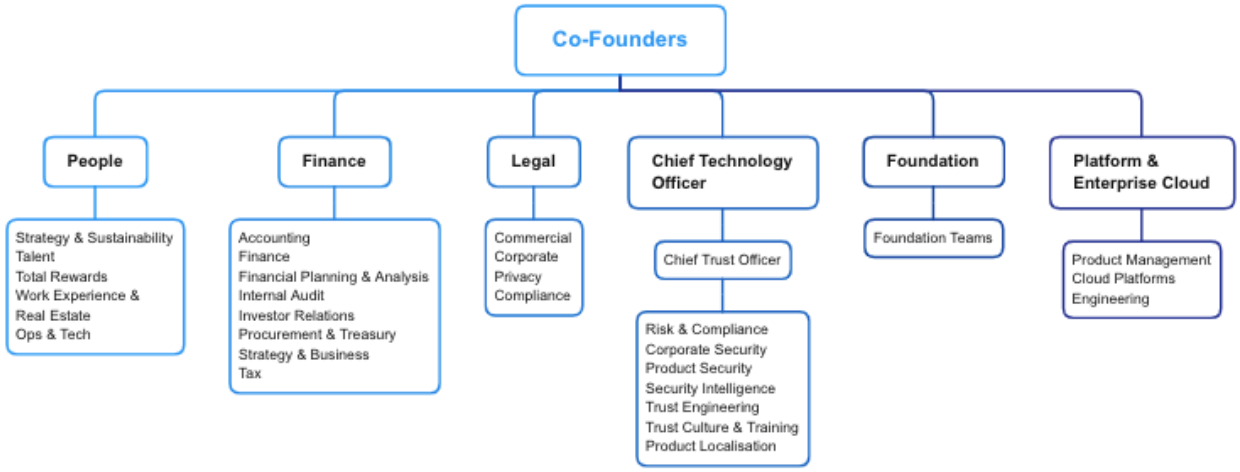

Figure 3: Atlassian's Organizational Chart

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 Platform and Enterprise Cloud, People, Foundation, Legal, Finance, and Technology teams. All teams have full responsibility for key operations within Atlassian. Refer to the People table above for more detail regarding the functions of each team.

Management's Philosophy and Operating Style

The control environment at Atlassian entails the involvement and ongoing engagement of Executive and Senior Management. The Risk and Compliance team engages the Executive and Senior Management in various ways:

- Standards – Atlassian follows specific standards that enable the organization to exercise practices around security, availability, quality, reliability, and confidentiality.
- Tools – Atlassian leverages tools designed specifically to assist in identifying, analyzing, tracking, deciding, implementing, and monitoring risks and findings. In addition, the tools allow the Company to effectively communicate and collaborate using workflows to help ensure activities are properly tracked. The use of customized tools allows them to be more closely integrated with the standard way of how Atlassian operates: specific, scalable, systematic, and robust.

- Enterprise Risk Management Process – Atlassian uses an Enterprise Risk Management process that is modeled after International Organization for Standardization (ISO) 31000:2009 "Risk Management – Principles and Guidelines."
- Unified approach – As Atlassian becomes involved across various best practices and legal and regulatory requirements, it becomes more essential to create control activities that are universal and not unique to specific standards and guidelines. Instead of tracking control activities specific to a standard, Atlassian tracks activities that are universal and meet multiple standards. This approach has enabled Atlassian to speak a common language across the organization. Along with a unified approach comes operational efficiency and a way to establish a controlled environment more effectively.

Human Resources Policies and Procedures

Atlassian has a job posting process and job advertisement template for all recruiters and team members to determine what needs to be included in each job advertisement. All Atlassian job ads are required to pass an approval process before they are posted on the careers page. The job ad is created by the recruiter and hiring manager. Additionally, a team reviews posted job ads for consistency, spelling/grammar, diversity-friendly verbiage, etc.

The recruiting process is based on prior relevant experience, educational background, and a clear understanding of integrity and ethical behavior. As part of the hiring process, interview feedback is collected in the applicant tracking system, Lever, for all candidates that participate in an onsite interview. Each interviewer, hiring manager, and HR member has access to Lever and can view the candidates' profiles. A recruiter will not initiate an offer for hire without receiving a minimum of one interview review in Lever prior to their start date. The exception to this process is contractors, interns, and graduates. For contractors, who are hired outside of the standard hiring process and outside of Lever, there is a confirmation screening step in the onboarding process within the Service Desk. For interns and graduates, a recruiting manager will approve the offer letters because of the bulk nature and timing of these hires.

Roles and responsibilities are documented in job ads as well as within the online applicant tracking system. Background checks are also performed, and results are reviewed against a results matrix and escalated to Legal and Head of HR Operations if needed. Background checks are performed by Atlassian for all full-time new hires. For contractors who are hired as part of an agency, background checks are not performed by Atlassian, but rather by the agency. Atlassian has a contract with all agencies to perform timely background checks and assess the results.

In addition, confidentiality and protection of company assets are clearly communicated and acknowledged by new hires. The HR Operations team delivers the plan to the employee during the onboarding communications process. Atlassian also requires that all employees and independent contractors sign a Confidential Information and Invention Assignment (CIIA) Agreement.

A weekly review is performed to determine that new employees have signed the CIIA, and that background checks are completed prior to their start date.

Once a year, Atlassian people leaders host performance check-ins with their team members to have a two-way conversation about how each team member contributed to Atlassian's success for the previous 12 months and to identify opportunities for improvement. After the check-in feedback process closes, the managers then provide performance and relative contribution ratings for all those on their team. The final stage of performance appraisals is Atlassian's salary planning process for providing potential merit increases.

Manual presentations, reminders, and training are used to communicate the process to Atlassian employees. In addition, the system controls provided by Workday (for check-ins and relative contribution and salary planning) track that all eligible Atlassian employees participate in performance reviews.

Communication and Information

Atlassian constantly updates the customers on their responsibilities as well as those of Atlassian. Communication includes but is not limited to policies, guidelines, security, product changes, and product alerts. Atlassian also communicates changes to security, availability, and confidentiality commitments to its customers, vendors, and internal users through the Atlassian website, when applicable.

Customer responsibilities are described on the Atlassian customer-facing website. The responsibilities include, but are not limited to, the following:

- Acceptable use policy
- Reporting copyright and trademark violations
- Customer agreement
- Designating customers as authorized users
- Guidelines for law enforcement
- Privacy policy
- Reseller agreement
- Professional services agreement
- Service-specific terms
- Third-party code in Atlassian products
- Training terms and policies
- Trademark

Atlassian uses the Atlassian Trust Center website to communicate the latest information on the security, reliability, confidentiality and compliance of its products and services. This includes communicating its membership to the Cloud Security Alliance and providing information on its compliance program and the various control standards it adheres to, such as ISO 27001.

In addition, customers and Atlassian internal users are offered multiple methods for contacting Atlassian to report bugs, defects, vulnerabilities, availability, security, and confidentiality issues.

Customer support (https://support.atlassian.com/) is the service desk where customers can submit requests for support from Atlassian. Customer issues are handled by Atlassian Support and escalated to engineering teams if needed.

- https://support.atlassian.com/halp/
- support@halp.com
- https://community.atlassian.com/
- https://plz.halp.com
- Intercom (live web chat)

Atlassian also communicates security, availability, and confidentiality criteria to the internal users through the onboarding process and policies and procedures available in the internal Confluence pages.

A description of the Halp system delineating the boundaries and describing relevant components is documented on the Atlassian intranet and the customer-facing website. Any significant changes made to the systems (new feature releases, integrations with other systems, interface updates) are also communicated to customers via the Atlassian customer- acing website. Blog posts generally include links to documentation and support resources that customers can use to troubleshoot issues and contact Atlassian. Availability of the Halp system, including the status and uptime, is published in the customer-facing website for all customers.

Risk Assessment and Mitigation

An Enterprise Risk Management (ERM) process is in place to manage risks associated with the Company strategy and business objectives. Atlassian utilizes a process that:

- Establishes the context, both internal and external, as it relates to the Company business objectives
- Assesses the risks
- Facilitates the development of strategies for risk treatment
- Communicates the outcome
- Monitors the execution of the risk strategies, as well as changes to the environment

The Enterprise Risk Management (ERM) process is modeled after ISO 31000-2009 "Risk Management – Principles and Guidelines."

An enterprise risk assessment is conducted annually, which includes key product stakeholders. When performing a risk assessment under the ERM framework, risk is considered holistically on its impact to the organization, not just to the individual function, department, or product that is directly impacted by the risk. While there may be specifics for a particular function, product, or service, risks are always considered in terms of affecting the entire company. This principle is followed, not only in the analysis but also in the evaluation of the risks (e.g., a risk that is critical for product A and low for Atlassian is evaluated as low). Nevertheless, if during the analysis a significant concern is discovered for a particular function, product, or service, this is flagged for subsequent follow-up.

To perform activities supporting the ERM, various sources of information are crucial to encompass all areas of the organization. Information sources include but are not limited to:

- Business goals and objectives – High-level business goals and objectives, and the strategies in place to achieve these goals and objectives.
- Major initiatives – Large projects and initiatives that could have a significant impact on the Company's risk profile. Additionally, Risk and Compliance managers are engaged by various teams, and they bring their knowledge of the environment into consideration.
- Risk and Compliance assessments – Throughout the year, Atlassian performs several periodic and ad-hoc assessments, which include assessments of key product stakeholders. Results of the assessments are captured in the Atlassian Governance, Risk, and Compliance (GRC) tool.
- Incidents – Atlassian utilizes a common Incident Management Process, including Post-Incident Review (PIR). The goal of PIR is not only to establish the root cause but also to create actions aimed at reducing the risk of repeated incidents.

- Organizational policies – Organizational policies that have been put in place to achieve the organization's strategic goals and objectives.
- Interviews with major stakeholders and subject matter experts (SME) – As part of the structured Enterprise Risk Assessment, Atlassian interviews all members of the Management team and engages with SMEs as needed.
- Other sources – Atlassian may consult industry publications, analyses, incidents, etc., as necessary.
- Internal and external context of the ERM process includes but is not limited to understanding the following:
  - Competitive environment – who Atlassian's major competitors are, what threat level they present, and what the trends in Atlassian's industry are
  - Legal/regulatory environment – what Atlassian's obligations are within their operating jurisdictions, what industry standards Atlassian needs to abide by
  - Financial environment – status and trends in the financial and currency markets that could affect Atlassian, perceptions, and values of external stakeholders
  - Technological environment – what the trends are in technology and software development
  - Business environment – markets that Atlassian is currently in or plans to enter, what the perception is of Atlassian and its products/services, what the current developments and trends in Atlassian's ecosystem are, major vendors, and customers
  - Human environment – what the social and cultural trends that could affect Atlassian are, what the status and trends are of the talent pools where Atlassian currently has or plans to establish presence
  - Natural environment – considerations related to natural disasters and office locations and facilities

The goal of establishing the external context is to identify potential key drivers and trends that could impact the organization.

- Organizational structure, governance, roles, and accountabilities
- Short- and long-term strategies, objectives, initiatives, programs, and projects
- Resources and capabilities (capital, people, skill sets, technologies, facilities)
- Operations (processes, services, systems)
- Organizational culture and values
- Information, information flow, and decision making
- Policies and standards
- Vendor agreements and dependencies

The goal of establishing the internal context is to identify potential key internal misalignments between strategy, objectives, capabilities, and execution.

The Risk and Compliance function plays a crucial role in Atlassian's ability to integrate ERM through the organization. The risk assessment process entails the following:

- Identification of risks
- Analysis of risks identified
- Evaluation of the risks
- Treatment of the risks

Throughout all stages of the ERM process, the Risk and Compliance team communicates with the relevant stakeholders and consults with appropriate subject matter resources.

All risks and associated treatment plans (e.g., mitigating actions) are recorded in the GRC tool. Links to detailed treatment plans, along with individual tasks, are also established. The Risk and Compliance team monitors the progress and provides oversight of the plan's execution. Progress review is part of the operational business function meetings, as well as periodic updates to the risk owners and executive operations.

The Atlassian Risk and Compliance team monitors the internal control environment and identifies significant changes that have occurred. The Risk and Compliance team meets to discuss:

- Risk and Compliance strategic direction

  Changes happening within the organization that affect Risk and Compliance efforts and initiatives
- Changes happening outside of Atlassian that affect Risk and Compliance efforts and initiatives
- The Risk and Compliance pipeline of how Atlassian approaches risk and compliance with internal customers
- Changes to existing and ingesting of new compliance standards

Entity Level Risk

A fraud risk assessment is performed annually by the head of Risk and Compliance. A cross-functional survey of employees in areas susceptible to fraud is conducted and combined with an evaluation of external risks. The results of the survey are consolidated into a report by an independent third-party company, which identifies and ranks areas of risk within the Company. The head of Risk and Compliance reviews the risks and recommendations and addresses them on a case-by-case basis. If needed, the recommendations will be added to Atlassian's ERM. The results are included in the enterprise risk assessment, which is communicated to the board and executive-level managers annually.

A whistleblower hotline is established and is accessible to both external individuals and employees within the Company. The whistleblower hotline is included within the Code of Conduct, which all employees are required to certify that they received. If an individual calls the whistleblower hotline, the General Counsel, Associate General Counsel, and audit committee chair receive a notification with the details of the claim. If a claim is received, it is discussed at the next audit committee meeting, including remediation action and resolution. To ensure that the whistleblower hotline notification system is operating properly, it is tested every six months.

Vendor Management

Atlassian has a formal framework for managing the life cycle of vendor relationships, including how Atlassian assesses, manages, and monitors its suppliers to ensure an appropriate control environment consistent with Atlassian's security, availability, and confidentiality commitments.

As part of the onboarding process, high-risk vendors are subject to a risk assessment and detailed review by internal Atlassian cross-functional SMEs. This involves evaluating the supplier's control environment and overall security posture based on information contained in supplier questionnaires, compliance reporting (e.g., System and Organization Controls [SOC] 2), and policies. Vendor agreements, including terms and conditions, and any commitments related to security, confidentiality, and availability, are also reviewed and signed prior to engaging with any vendor.

Mitigating, resolving, or accepting any risks that were identified during the due diligence process is handled and documented by the appropriate cross-functional SMEs and designated Atlassian reviewers and approvers.

Additionally, Atlassian evaluates high-risk vendors at least annually for ongoing compliance with key processes and their contractual obligations to achieve security, availability, and confidentiality commitments. The Risk and Compliance team obtains, at a minimum, the current compliance reporting of each vendor (e.g., SOC 2 report, ISO 27001 certificate) and evaluates the results included in the report to determine if controls are sufficient to achieve Atlassian's principal service commitments and system requirements. Any exceptions are assessed to determine the potential impact to the Atlassian control environment.

Information Security

Information and information systems are critical to the operations of Atlassian globally. Atlassian takes all appropriate steps to safeguard and properly protect company information, customer information, and information systems from threats such as error, fraud, industrial espionage, legal liability, and natural disaster.

Information Security Controls

Information security controls are defined as appropriate and compliance with the controls is reviewed by Atlassian's Risk and Compliance team.

Periodic Review of Risks and Controls

The Atlassian security program seeks to balance risk against the cost of implementing controls. A periodic review of risks and security controls will be carried out to address changing business requirements and priorities. All security policies are assessed and reviewed at least annually. Evaluation of risks and controls is accomplished in line with a Risk Management Program and Compliance Program.

Information Security Training

Appropriate training enables employees to comply with their responsibilities as it relates to the Information Security Policy.

All Atlassian employees (including contractors) are subject to mandatory annual user awareness training. Employees are given 30 days to complete the training. This training is managed and tracked on the corporate learning platform to ensure organization-wide completion.

Disciplinary Notice

In the event of a violation of the Information Security Policy, employees are required to notify management upon learning of the violation. Employees who violate the Information Security Policy are subject to disciplinary action, up to and including termination of employment.

Monitoring

The Halp Engineering team continuously monitors a vast array of system metrics from across the infrastructure and application performance metrics. In addition to metrics, a large volume of log information is captured from the various services that support Halp as a product. Metrics, logs, and frequent automated system checks are combined into an overall monitoring solution that sends automated alerts when collected data points exceed predefined thresholds. Alerts are sent to the Engineering team when exceptions are identified. These alerts notify the Halp Engineering team of any potential incidents for remediation.

The availability status of Halp is published online together with details of historical incidents that have impacted availability.

Technical Vulnerability Management

Technical vulnerability management utilizes a variety of sources to identify vulnerabilities and track them to resolution.

Vulnerabilities from all sources are tracked via the Vulnerability Funnel Jira project and are reviewed and resolved according to Atlassian's Security Service-Level Objectives (SLO) time frames. The Vulnerability Funnel automation notifies the appropriate system or application owner of new security vulnerabilities, sends multiple notifications as the vulnerability approaches its due date, and reports on issues not remediated by the due date to leadership.

Technical vulnerabilities in Atlassian products and systems are identified via the following methods:

- Host-based vulnerability scanning
- Cloud configuration monitoring
- Software composition analysis (SCA)
- Vulnerabilities identified internally by security reviews or engineering teams
- External reports from security researchers via Atlassian public bug bounty program
- External reports from customers via Atlassian Support
- External reports via email

Regular reviews of all identified Atlassian critical vulnerabilities are conducted daily when applicable, and SMEs monitor the vendor mailing list for notification of new versions and vulnerabilities.

Atlassian uses vulnerability scanning tools to scan the internal- and external-facing network, as well as configurations in AWS. Results are emailed to the relevant system owner for triaging and, if the system owner determines it to be necessary, creating a ticket for resolution.

Penetration Testing

Atlassian products are required to participate in a public bug bounty program. Submissions are initially triaged by Bugcrowd for validity and reproducibility. Valid submissions are then released into Atlassian's bug bounty account and triaged by the Security team and assigned a priority level. Jira tickets are then raised in a central project, assigned to the relevant system owner, and tracked to resolution.

Endpoint Protection and Asset Management

Atlassian's Windows and Mac machines utilize Active Directory for authentication. Atlassian uses a standard build as a guide when provisioning or re-provisioning new machines with enabled drive encryption and uses Crowdstrike for malware protection.

Ongoing workstation asset management, security patch deployment, password protection, screensaver/screen lock settings, and drive encryption auditing are done using policies deployed through Workspace One (Windows) and Jamf Pro (Mac) asset management software.

Email Scanning

Google Workspace and Proofpoint are used to provide malware protection for incoming email at the perimeter. In addition, on an annual basis, Atlassian provides security training to educate staff on various security risks and best practices, including those associated with email phishing.

ZeroTrust Network

Atlassian has implemented a ZeroTrust network, of which the basis of this infrastructure is to only allow access from known devices that are enrolled into a management platform. Regular reconfirmation of the enrollment status is performed. Endpoints are placed into a tiered network (High, Trusted, Open) based on their security posture and type of device. This placement determines the level of access to services.

Additionally, firewalls are maintained at the corporate network edges, for platform and non-platform-hosted services, and for its shared Amazon VPC. All devices are configured via security policy rules, and maintenance is conducted by the associated internal teams (e.g., corporate – Workplace Technology [WPT], platform – Micros, non-platform – Product teams, Amazon VPC – Network Engineering). To access the production environments, users must be authenticated to the Atlassian network (via the corporate office network or virtual private network [VPN]), therefore enforcing protection by the firewalls.

Firewall rules are in place to restrict access to the production environment, and only authorized users of designated Active Directory groups can change permissions to firewall rules.

Encryption

Customer data is encrypted at rest, and external connections to Halp are encrypted in transit via the TLS 1.2 protocol. Atlassian monitors the certificate-authority-issued TLS certificates and renews them prior to expiry.

Internal and External Audit

The Internal Audit team conducts internal audits relating to Sarbanes-Oxley 404 (SOX), SOC 2, ISO, and operational audits. The results are communicated, and corrective actions are monitored to resolution.

Atlassian also engages external auditors to perform compliance audits against various standards at least annually. The results of the audits are captured as findings in the GRC tool, reported to management and the audit committee, and tracked to resolution.

Control Activities

Logical Access

Customer Production Accounts

Provisioning Customer Production Accounts

When creating an account with any of Atlassian's products, the user is directed to acknowledge the standardized customer agreement online, which also defines the customer's responsibility around security, availability, and confidentiality. An account cannot be made for any of Atlassian's products without the customer first being directed to acknowledge the customer agreement. Any updates to the customer agreement are reviewed and approved by the Legal department.

There are also agreements Atlassian has between Solution Partners and Global Alliance Partners ("Partners"), where Partners can join a program to resell Atlassian's offerings. For customers who purchase directly through a Partner, customers' access to and use of the offerings is subject to the applicable customer agreement. Partners are responsible for ensuring each customer has entered such customer agreement, at or before such customer's purchase or use of the offerings, in a manner that is legally binding upon the customer. From time to time, based on the proposed deal size, Atlassian legal may negotiate a master services agreement with certain Enterprise customers.

After the customer acknowledges the customer agreement, the customer account is provisioned, and an account owner is assigned. Unique identifiers are assigned to customers upon creation, which logically segregates data from other accounts.

De-provisioning Customer Production Accounts

Customers can request for their data to be deleted via a support ticket or via the Halp Slack Channel. Upon doing so, Halp Support will validate the scope, time frame, and legitimacy of the request, and if warranted, Engineering will facilitate the deletion. Engineering has crafted a set of tools to perform deletions safely and consistently.

Upon deletion of a user's account in Halp (by the user themselves, or their organization's administrator in the case of enterprise accounts), all data regarding that user account is permanently erased within a reasonable period.

Production Environment Access

Customer Access

External users can register for a Halp account using their Slack or Microsoft Teams account. Customers are responsible for managing access to their own instances. Users with an administrator role within the instance can add and remove user accounts. Users can only access instances they are authorized to.

Atlassian Internal Users Access

Access to the Halp production environment is tightly restricted and is provisioned based on the principle of least privilege. Access can only be gained from within the Atlassian network or while connected to the corporate VPN and requires two-factor authentication via Duo. Additionally, Atlassian users must connect to a jump box and must have a valid key to gain SSH access.

Password

Customer Access

To login to Halp, users need to authenticate to Slack or Microsoft Teams. Halp is connected to Slack and Microsoft Teams via OAuth 2.0. OAuth is used for authorizing secure access to external applications without providing them with the account's password. Halp does not store any passwords, and customers can revoke OAuth tokens at any time.

It is the customers' responsibility to ensure that their accounts are appropriately configured and set up to their corporate network/password and other authentication mechanisms such as OAuth.

Atlassian Internal Users Access

Passwords are an important part of Atlassian's efforts to protect its technology systems and information assets by helping ensure that only approved individuals can access these systems and assets.

Atlassian provides various secured methods to connect to Atlassian resources. The primary method for connecting to Atlassian resources is via the Idaptive SSO system, which requires two-factor authentication.

Duo two-factor authentication is also required when logging into VPN. The only exception is certain Internet Protocol (IP) addresses that are whitelisted within the “exempt IP” settings in Idaptive.

For Atlassian employees, a minimum of 12 characters is enforced for passwords in Idaptive as configured in Atlassian's Active Directory.

User Provisioning, Review, and De-provisioning of Atlassian Internal Users

Atlassian Internal User Provisioning

Active Directory contains a subset of groups which are automatically created and maintained based on demographic and employment information in the HR Workday system. These groups are based on division, team, location, employment type, and management status. As well as initially provisioning membership, staff members’ assigned groups will be updated to reflect a team/department change or termination. Active Directory group membership is automatically assigned based on the user's department and team.

Access to the Atlassian internal network and internal tools is restricted to authorized users via logical access measures:

- Each Atlassian user account must have an Active Directory account.
- Each Atlassian user account must be a member of the appropriate Lightweight Directory Access Protocol (LDAP) group.

Access to the AWS production environment, databases, and supporting tools in addition to the Workday group access is provisioned only after appropriate approval via a Jira ticket.

Atlassian Internal User De-provisioning

De-provisioning of access via terminations are initiated at the Workday level. HR initiates the termination once notified by management via Workday. The system does not permit termination dates to be backdated. Idaptive is configured to pull all the upcoming terminations from Workday via a job and then schedules the user to be terminated accordingly in Active Directory (within eight hours). Once terminated via the above process, users are unable to manually connect to the network, log in to the Wi-Fi, or access via VPN, including remote access via Duo and access to Halp’s back-end systems. Additionally, any access to systems that are not managed via Active Directory is manually revoked.

Atlassian Internal User Role Changes

Role changes are a common practice, and Atlassian has a process in place to make any internal transition an effortless and seamless event. When a user changes roles and moves from the Engineering, Support, or Finance group to one of the other areas (Engineering, Customer Support & Success, or Finance groups), an alert is generated and a notification is sent to the HR information systems manager or WPT team, who are responsible for performing the access review, and for helping ensure timely modification of system access, commensurate with the new role.

Atlassian Internal User Access Reviews

Atlassian’s Engineering managers or team leads perform semi-annual privileged user access reviews of Halp and the associated in-scope supporting tools and services. Any discrepancies identified are escalated to the respective managers and are addressed in a timely manner based on the nature of remediation required.

Privileged access to Workday is limited to appropriate users. The People Central Systems Support Specialist performs a review of Workday administrator users semiannually.

Access of Atlassian Support Team to User Data

Halp has a dedicated group of Halp customer support personnel who help customers troubleshoot issues while using Halp. The support personnel use Retool to provision temporary access to customers' instances. Customer instances are only accessed whenever there is a valid customer support request. The ability to initiate an impersonation request is limited to support personnel. Access to Retool is formally requested and approved and is reviewed semiannually.

Hosting Facilities

Halp is hosted in AWS facilities and utilizes MongoDB, which is also hosted on AWS. Atlassian reviews the SOC 2 report of all material vendors (including infrastructure providers) annually to assess the adequacy of the vendor's controls in meeting Atlassian's security, availability, and confidentiality commitments. Any issues identified as part of the review are followed up on and addressed as necessary.

System Operations

Incident Management

An organizational wide incident management process is in place. The incident management process must meet the Atlassian Incident Management Standard.

The focus of all incident management is to minimize downtime, service degradation, or security risk for customers and internal users. Every action in managing an incident is recorded in an Incident Management System under an incident ticket.

The standard principles of incident management consist of the following:

- Detection and Recording – Atlassian has the appropriate tools in place to properly detect and record all incidents.
- Incident Classification for Resolution and Communication – Incidents are classified according to the level of severity. Incident Managers are a crucial part of exercising judgment on the incident priority.
- Communication Steps Based on Severity – The severity of the incident determines the communication steps all Incident Managers take.
- Investigation and Diagnosis – Investigations begin with existing runbooks and other relevant documentation. Many incidents have pre-formulated solutions captured in runbooks.
- Resolution and Recovery – The Incident Management team encourages quick and responsive incident resolution and can resolve incidents immediately.
- Incident Handover – When incidents are escalated and run longer, incident handovers are coordinated.
- Closure and PIR – Clients and customers can provide feedback on the resolution of the incident. Support or customer advocacy confirms the resolution of all customer-reported incidents with the reporting customer. When the incident is completely resolved, the Incident Manager completes and closes all incident records and tickets. After high severity incidents, the Incident Manager completes a PIR, which is to be documented. If the root cause is fully understood from a previous incident, then the PIR can link to that previous incident.
- Incident Reporting and Analysis – Data from IT incidents, including those received and resolved by Support, are typically analyzed and reported for trends and indications of unidentified problems requiring definition and resolution.

- Relation to Problem Management – Where possible, all related or similar incidents are examined for a common cause. Where incidents temporarily cannot be associated with any root cause (problem), they are reviewed for any other common incidents.

Severity Levels		
Severity	**Description**	**Examples**
0	Crisis incident with maximum impact	• Major security incident • Customer data loss
1	Critical incident with very high impact	• Outage to the products affecting all users for over one hour • Issue affecting critical functionality for all the product users
2	Major incident with significant impact	• Outage to Atlassian's internal extranet for over one hour
3	Minor incident with low impact	• Degraded plugin affecting 10 cloud customers of a specific product

Factors considered when determining severity:

- Length/duration of an outage – If the rough time it will take to complete an incident is known, Atlassian uses this to help gauge the severity of an incident. Typically, incidents with no known estimated duration will take higher severity levels.
- Number of customers affected – This assessment is made based on the volume of customer tickets and the percentage of traffic that is impaired or impacted.
- Customer/internal service – Customer services fields requests that come in through support.atlassian.com.
- Data loss – Any potential data loss to customers increases severity.
- Security risks/breach – If a security breach has been made public, if customer confidentiality has been compromised, or if Atlassian is in violation of the terms of a contractual agreement, these are usually severity 0 if active compromise has occurred.
- Down or degraded – If a service or tool is degraded, how degraded? For example, Atlassian products being slow might be a lot more impactful than a slow response from https://support.atlassian.com.

Change Management

Change Initiation

Changes to Halp and its supporting utilities and services are planned by the product development teams, which include product management, design, engineering, and quality assurance.

Change Development

Atlassian uses an agile development methodology to manage tasks within team-based development environments. The Halp products use an internally developed platform-as-a-service (PaaS), which provides controlled, common solutions for microservices such as deploying the service to machines, provisioning databases, configuring load balancing, and creating Domain Name System (DNS) records.

Halp and its supporting services each have a master source code repository (or master branch) where developers make changes. The branch holds the master copy of source code for developers to work on. Whenever a change is needed, a developer creates a local branch in Bitbucket, downloads the branch to their local drive and begins coding. After the code is updated, the developer creates a pull request to merge the code to the master branch.

Atlassian uses the "merge checks" feature built into Bitbucket to enforce peer review(s) and approval(s) and automated tests (green build tests) before the code can be merged. Before a pull request can be merged to the master branch, it must be approved by at least one authorized reviewer. Bitbucket prevents pull requests from being approved by the same user who requests it. This prevents any direct changes to the master branch except through a peer-reviewed pull request that has undergone successful testing.

If there are any changes to the code contained in the pull request, any previous approvals are removed, and the pull request must be re-approved before it can be merged.

An Atlassian-only "Compliance" setting in Bitbucket prevents any of the above controls from being changed or turned off. If the "Compliance" setting itself is turned off for a repository, Bitbucket logs an event to the Atlassian data warehouse, where it triggers an automated alert in the REPCOM system. The alerts are routed to the relevant development manager to confirm that no unauthorized changes were made and to restore the setting. The manager of the personnel making the change is automatically tagged as an “Assigned” to the Jira ticket to the responsible manager, who is responsible for:

- Investigating the reason for the settings alteration and commenting on the ticket
- Confirming that the settings are re-enabled (if applicable)
- Resolving the ticket after the settings have been re-enabled (if applicable)

Change Deployment

After a pull request is merged into the production branch and the team is ready to deploy the new version, the deployment is executed via the authorized build system. Before a build can be created, the build system performs a check to confirm that the appropriate controls as described above were in effect on the source code repository. If it identifies that the controls are not implemented, it automatically prevents the builds from being deployed.

Only artifacts built by the authorized build system can be deployed to the Halp production environment. Any artifact deployed by another source is automatically rejected.

Customers are notified of any major release through the customer-facing website.

Scanning of Production Code

Halp utilizes vulnerability scanning tools to continuously scan and review the code base to detect vulnerable open-source libraries being used. The scanner is integrated into the Halp build plan and is run automatically when changes are made to the code base. Tickets are created automatically when vulnerabilities are detected. Developers review the reports, assess the vulnerabilities, determine the risk and severity level, and triage the findings based on severity level. Different levels of severity will be addressed and prioritized within the development ticket tracking system. All vulnerabilities are reviewed and actioned if required.

Deployment Script Changes and Infrastructure Changes

Other types of changes, such as critical infrastructure changes (e.g., operating system, configurations) and changes to the deployment script, follow the same change management process outlined above.

Emergency Changes

Emergency changes follow an expedited process, meaning that change management controls are still adhered to.

Availability

Capacity Management

A Capacity Planning program helps Atlassian determine what the current and future resource (people and technology) needs are to meet customer expectations of the goods and services being delivered. The infrastructure and systems that make up Halp are continuously monitored for utilization levels and adjusted accordingly. Halp stakeholders monitor infrastructure capacity and adjust resizing and reconfiguring of systems based on real-time load, to ensure that the systems are provisioned with enough headroom to handle surges and spikes of user activity, as well as for load sharing.

Capacity planning is performed on a perpetual basis to help ensure projections are accurate and complete. Capacity planning is in place to better meet customer needs, to help ensure compute and capacity resources are optimized, and to help forecast set capital expenditure.

Backup and Replication

Backups

MongoDB creates and saves automated backups of the databases every hour and backups are tested for data recoverability quarterly.

Replication

Atlassian uses MongoDB as its primary database and Amazon S3 to manage customer attachments. MongoDB is responsible for providing high availability and failover support for database instances using multi-AZ deployments. In a multi-AZ deployment, MongoDB is responsible for automatically provisioning and maintaining a synchronous standby replica in a different AZ of the same region to provide data redundancy and failover capability. Halp MongoDB databases are all set up as multi-AZ. This multi-AZ replication is managed by MongoDB, including replication issue resolution.

Disaster Recovery

A disaster recovery policy is in place and is reviewed annually by the disaster recovery steering committee. Procedures for disaster recovery execution are defined, reviewed, tested, and in place. The policy describes, at a high level, the purpose, objectives, scope, critical dependencies, recovery time objective/ recovery point objective (RTO/RPO), and roles/responsibilities. Atlassian follows “ISO 22301 Business Continuity” as a guideline for their disaster recovery program.

Disaster recovery tests are performed quarterly and are performed in a simulated environment. Tabletop exercises are also performed to help disaster response teams walk through various scenarios of incidents. After disaster recovery tests are performed, outputs of the tests are captured, analyzed, and discussed to determine the scope of the next steps for continuous improvement of the tests. The improvement efforts are captured within engineering tickets and followed through as appropriate.

Confidentiality

All Atlassian employees share in the responsibility to safeguard information with an appropriate level of protection by observing the Information Classification Policy:

- Information should be classified in terms of legal requirements, value, and criticality to Atlassian
- Information should be labeled to manage appropriate handling

- Manage all removable media with the same handling guidelines as below
- Media being disposed of should be securely deleted
- Media containing company information should be protected against unauthorized access, misuse, or corruption during transport

Data Classification		
Rating	**Description**	**Examples**
Public	Information that is freely available to the public.	• Any information available to the public • Released source code • Newsletters • Information up on website
Internal	Information internal to Atlassian that would be embarrassing if released, but not otherwise harmful. This is the default classification for most Atlassian-generated information.	• Most extranet pages • Jira issues such as invoices or phone records • Unreleased source code • Information only accessible from the office IP addresses • Product announcements before the release date
Confidential	Information that Atlassian holds that could cause damage to Atlassian and/or its customers if released. This is the default for any information customers have provided to Atlassian.	• Customer support issues logged on support site • Business plans and deals (including on the extranet) • Information under a nondisclosure agreement • Unresolved security issues in Atlassian's products • Third-party closed-source code • Most passwords • Customer source code or other intellectual property (IP) stored in Atlassian's hosted products
Restricted	Information that customers and staff have trusted to Atlassian's protection that would be very damaging if released. Trust is the operative word.	• Customer personally identifiable information (PII) • Customer credit cards data • US Social Security numbers (customer or staff) • Staff personal, bank, and salary details • Sensitive company accounting data • Decryption keys or passwords protecting information at this level • Any other data Atlassian has a strong legal or moral requirement to protect

Complementary User Entity Controls (CUECs)

The Company's controls related to Halp cover only a portion of overall internal control for each user entity of Halp. It is not feasible for the service commitments, system requirements, and applicable criteria related to the system to be achieved solely by the Company. Therefore, each user entity's internal control should be evaluated in conjunction with the Company's controls and the related tests and results described in Section 4 of this report, taking into account the related CUECs identified for the specific criterion. In order for user entities to rely on the controls reported herein, each user entity must evaluate its own internal control to determine whether the identified CUECs have been implemented and are operating effectively.

The CUECs presented should not be regarded as a comprehensive list of all controls that should be employed by user entities. Management of user entities is responsible for the following:

Criteria	Complementary User Entity Controls
CC2.1	• Customers are responsible for identifying approved points of contacts to coordinate with Atlassian. • Customers are responsible for the security and confidentiality of the data submitted on Atlassian support tickets.
CC2.3	• Customers are responsible for assessing and evaluating any potential impact add-ons may have on their instance.
CC6.1	• Customers are responsible for configuring their own instance, including the appropriate set-up of their logical security (such as IP allow-listing, two-factor authentication, and SSO setup), privacy, and security settings. • Customers are responsible for safeguarding their own account access credentials, including passwords or API keys and tokens.
CC6.2 CC6.3	• Customers are responsible for managing access rights, including privileged access. • Customers are responsible for requesting, approving, and monitoring Atlassian's customer support access to their account.
CC6.2 CC6.3 C1.2	• Customers are responsible for requesting that their accounts be removed.
CC6.6 CC6.7 CC6.8	• Customers are responsible for ensuring that their machines, devices, and network are secured.
CC7.3	• Customers are responsible for alerting Atlassian of incidents (related to security, availability, and confidentiality) when they become aware of them.

Subservice Organizations and Complementary Subservice Organization Controls (CSOCs)

The Company uses AWS and MongoDB as subservice organizations for data center colocation services. The Company's controls related to Halp cover only a portion of the overall internal control for each user entity of Halp. The description does not extend to the colocation services for IT infrastructure provided by the subservice organizations. Section 4 of this report and the description of the system only cover the Trust Services Criteria and related controls of the Company and exclude the related controls of AWS and MongoDB.

Although the subservice organizations have been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organizations. CSOCs are expected to be in place at AWS and MongoDB related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. AWS and MongoDB physical security controls should mitigate the risk of unauthorized access to the hosting facilities. AWS and MongoDB's environmental protection controls should mitigate the risk of fires, power loss, climate, and temperature variabilities.

Company management receives and reviews the AWS and MongoDB SOC 2 reports annually. In addition, through its operational activities, Company management monitors the services performed by AWS and MongoDB to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organizations to monitor compliance with the service agreement, stay informed of changes planned at the hosting facilities, and relay any issues or concerns to AWS and MongoDB management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to Halp to be achieved solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls and related tests and results described in Section 4 of this report, taking into account the related CSOCs expected to be implemented at AWS and MongoDB as described below.

Criteria	Complementary Subservice Organization Controls
CC6.1	• AWS and MongoDB are responsible for ensuring that IT access above least privileged, including administrator access, is approved by appropriate personnel prior to access provisioning. • AWS and MongoDB are responsible for privileged IT access reviews. • AWS and MongoDB are responsible for timely revocation of user access upon termination. • AWS is responsible for encrypting data at rest and in transit.
CC6.4	• AWS is responsible for restricting physical access to the computer rooms, which house the entity's IT resources, servers, and related hardware to authorized individuals through a badge access system or the equivalent and for ensuring that such computer rooms are monitored by video surveillance. • AWS is responsible for approving requests for physical access privileges from authorized individuals. • AWS is responsible for requiring visitors to be signed in by an authorized workforce member before gaining entry and to be escorted at all times.
CC6.5 CC6.7	• AWS is responsible for securely decommissioning and physically destroying production assets in its control.
CC7.1 CC7.2 CC7.3	• AWS is responsible for implementing and monitoring electronic intrusion detection systems that can detect breaches into data center server locations. • AWS is responsible for documenting procedures for the identification and escalation of potential security breaches.
CC7.2 A1.2	• AWS and MongoDB are responsible for installing environmental protections that include the following: cooling systems, battery and generator backups, smoke detection, and dry pipe sprinklers. • AWS and MongoDB are responsible for monitoring the environmental protection equipment for incidents or events that impact assets.
CC8.1	• AWS and MongoDB are responsible for ensuring that changes are authorized, tested, and approved prior to implementation.

Specific Criteria Not Relevant to the System

There were no specific security, availability, or confidentiality Trust Services Criteria as set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria) that were not relevant to the system as presented in this report.

Significant Changes to the System

There were no changes that are likely to affect report users' understanding of how Halp is used to provide the service from October 1, 2021 to September 30, 2022.

Report Use

The description does not omit or distort information relevant to Halp while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to their own particular needs.

Section 4

Trust Services Criteria, Related Controls, and Tests of Controls Relevant to the Security, Availability, and Confidentiality Categories

Control Environment Elements

The control environment represents the collective effect of various elements in establishing, enhancing or mitigating the effectiveness of specific controls. The control environment elements as described in the description of the system include, but are not limited to, the Code of Conduct, Policies and Procedures, and Human Resources.

Our tests of the control environment included the following procedures, to the extent we considered necessary; (a) an inspection of Atlassian's organizational structure including segregation of functional responsibilities and policies and procedures; (b) inquiries with management, operations, administrative, and other personnel who are responsible for developing, ensuring adherence to and applying controls; (c) observations of personnel in the performance of their assigned duties; and (d) inspection of documents and records pertaining to controls.

Description of Tests Performed by Coalfire Controls, LLC

Our tests of operating effectiveness of controls included such tests as were considered necessary in the circumstances to evaluate whether those controls, and the extent of compliance with them, were sufficient to provide reasonable, but not absolute, assurance that the trust services security, availability, and confidentiality categories and criteria were achieved throughout the period October 1, 2021 to September 30, 2022. In selecting particular tests of the operating effectiveness of the controls, we considered (i) the nature of the controls being tested; (ii) the types of available evidential matter; (iii) the nature of the criteria to be achieved; (iv) the assessed level of control risk; and (v) the expected efficiency and effectiveness of the test. Such tests were used to evaluate fairness of the presentation of the description of Atlassian's Halp System and to evaluate the operating effectiveness of specified controls.

Additionally, observation and inspection procedures were performed as it relates to system generated reports, queries, and listings within management's description of the system to assess the completeness and accuracy (reliability) of the information utilized in the performance of our testing of the control activities.

Trust Services Criteria, Related Controls, and Tests of Controls Relevant to the Security, Availability, and Confidentiality Categories

Control Environment			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC1.1	The entity demonstrates a commitment to integrity and ethical values.		
HR-3	Background checks are performed prior to an employee's start date. Results are reviewed against a results matrix and escalated to Legal and the Head of HR Operations if needed.	Inspected background check completion evidence for a sample of new employees to determine that background checks were performed prior to their start date and that the results were reviewed against a results matrix and escalated to Legal and Head of HR Operations if needed.	No exceptions noted.
HR-4	Employees and contractors are required to sign CIIAs as part of the onboarding process.	Inspected signed confidentiality agreements for a sample of employees and contractors onboarding during the period to determine that CIIAs were signed prior to start date.	No exceptions noted.
HR-5	Employees and contractors acknowledge the Code of Conduct annually.	Inspected the Code of Conduct to determine that it described employee and contractor responsibilities and expected behavior regarding data and information system usage.	No exceptions noted.
		Inspected acknowledgements for a sample of employees and contractors to determine that employees and contractors acknowledged that they had read and agreed to the Code of Conduct.	No exception noted.

Control Environment			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
HR-6	A weekly review is performed to determine that the CIIA and background checks are completed for new employees prior to their start date.	Inspected weekly review documentation for a sample of weeks to determine that a weekly review was performed to determine that the CIIA and background checks were completed for new employees prior to their start date.	No exceptions noted.
HR-7	Performance appraisals are performed at least annually	Inspected performance appraisal documentation for a sample of employees to determine that performance appraisals were completed by management during the period.	No exceptions noted.
HR-10	The Company has documented disciplinary actions in a formalized sanctions policy for employees and contractors who violate the Code of Conduct.	Inspected the Code of Conduct to determine that the Company had documented disciplinary actions in a formalized sanctions policy for employees and contractors who violated the Code of Conduct.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.		
ELC-4	The Audit Committee Charter defines the roles, responsibilities, and key activities of the audit committee.	Inspected the Audit Committee Charter to determine that the Audit Committee Charter defined roles, responsibilities, and key activities of the audit committee.	No exceptions noted.
ELC-5	The process of identifying and reviewing the Board of Director Candidates is defined in Nominating and Corporate Governance Committee charter.	Inspected the Nominating and Corporate Governance Committee Charter to determine that the process of identifying and reviewing the Board of Director Candidates is defined in the Nominating and Corporate Governance Committee charter.	No exceptions noted.

Control Environment			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
ELC-7	An Audit Committee meeting calendar and general meeting agenda are developed.	Inspected the Audit Committee meeting minutes for a sample of quarters to determine that the Audit Committee meeting calendar and general meeting agenda were developed.	No exceptions noted.
ELC-8	At least annually, the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation, and Leadership Development) review committee charters and corporate governance which define their roles, responsibilities, meeting frequency, participants, member qualifications and discussion topics	Inspected the board of directors meeting minutes to determine that the board of directors met during the period and its various subcommittees reviewed committee charters and corporate governance that defined roles, responsibilities, meeting frequency, participants, member qualifications and discussion topics.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		
ELC-1	The organizational charts are reviewed by appropriate Atlassian management and updated semi-annually.	Inspected review documentation for a sampled organizational chart review to determine that the organizational charts were reviewed by appropriate Atlassian management and updated semi-annually.	No exceptions noted.
ELC-2	Organizational charts are updated based on employee action notices and are available to all Atlassian employees via Workday.	Inspected the organizational charts to determine that they are updated based on employee action notices and available to all Atlassian employees via Workday.	No exceptions noted.

Control Environment			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
ELC-5	The process of identifying and reviewing the Board of Director Candidates is defined in Nominating and Corporate Governance Committee charter.	Inspected the Nominating and Corporate Governance Committee Charter to determine that the process of identifying and reviewing the Board of Director Candidates is defined in the Nominating and Corporate Governance Committee charter.	No exceptions noted.
ELC-14	Management has established defined roles and responsibilities to oversee the implementation of the security and control environment.	Inspected the information security policy to determine that management had established defined roles and responsibilities to oversee the implementation of the security and control environment.	No exceptions noted.
HR-1	The hiring manager reviews and approves job descriptions.	Inspected job descriptions for a sample of employees supporting the service to determine that job descriptions were documented, reviewed, and approved by the hiring manager, and included authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
HR-1	The hiring manager reviews and approves job descriptions.	Inspected job descriptions for a sample of employees supporting the service to determine that job descriptions were documented, reviewed, and approved by the hiring manager, and included authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	No exceptions noted.

Control Environment			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
HR-2	Job offers to external candidates are approved prior to hiring.	Inspected approval documentation for a sample of new hires to determine that job offers to external candidates are approved prior to hiring.	No exceptions noted.
HR-7	Performance appraisals are performed at least annually	Inspected performance appraisal documentation for a sample of employees to determine that performance appraisals were completed by management during the period.	No exceptions noted.
HR-8	Training is available to employees to support their continued development and growth.	Inspected training tools made available to all employees to determine that training is available to employees to support their continued development and growth.	No exceptions noted.
HR-9	User awareness training is performed at least annually for employees and contractors as part of the Atlassian Security Awareness program.	Inspected training completion evidence for a sample of employees and contractors to determine that user awareness training was performed at least annually as part of the Atlassian Security Awareness program.	Exception noted. For 3 of 44 employees and contractors sampled, user awareness training was not completed during the period.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
HR-1	The hiring manager reviews and approves job descriptions.	Inspected job descriptions for a sample of employees supporting the service to determine that job descriptions were documented, reviewed, and approved by the hiring manager, and included authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	No exceptions noted.

Control Environment			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
HR-5	Employees and contractors acknowledge the Code of Conduct annually.	Inspected the Code of Conduct to determine that it described employee and contractor responsibilities and expected behavior regarding data and information system usage.	No exceptions noted.
		Inspected acknowledgements for a sample of employees and contractors to determine that employees and contractors acknowledged that they had read and agreed to the code of conduct upon hire.	No exceptions noted.
HR-7	Performance appraisals are performed at least annually	Inspected performance appraisal documentation for a sample of employees to determine that performance appraisals were completed by management during the period.	No exceptions noted.
HR-10	The Company has documented disciplinary actions in a formalized sanctions policy for employees and contractors who violate the code of conduct.	Inspected the code of conduct to determine that the Company had documented disciplinary actions in a formalized sanctions policy for employees and contractors who violated the code of conduct.	No exceptions noted.

Communication and Information			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		
MTR-2	Continuous internal and external network vulnerability scanning is performed over the Atlassian environment. Vulnerabilities are reviewed, prioritized, and resolved as per the defined time frame.	Inspected continuous internal and external network vulnerability scan configurations to determine that internal and external network vulnerability scans were performed continuously to identify, quantify, and prioritize vulnerabilities.	No exceptions noted.
		Inspected remediation documentation for a sample of vulnerabilities identified during the period to determine vulnerabilities were resolved within Atlassian's standard resolution time frames.	No exceptions noted.
MTR-6	A log management tool is utilized to identify trends that may have a potential impact on the Company's ability to achieve its security objectives and generates alerts when specific events occur.	Inspected the log management tool configurations to determine that a log management tool was utilized to identify trends that may have had a potential impact on the Company's ability to achieve its security objectives and generated alerts when specific events occurred.	No exceptions noted.
RM-4	Internal audits are performed annually and results are communicated to management and the Audit Committee. Corrective actions are monitored.	Inspected internal audit documentation and test results to determine that internal audits were performed during the period and that the results were communicated to management and the Audit Committee, and corrective actions were monitored.	No exceptions noted.

Communication and Information			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
ELC-10	The Executive team sets strategic operational objectives annually.	Inspected strategy and planning documentation to determine that the Executive team set strategic operational objectives during the period.	No exceptions noted.
ELC-12	Atlassian has established a Whistleblower hotline that is accessible to both external individuals and employees within the Company	Inspected the Whistleblower hotline communication channels to determine that Atlassian had established a Whistleblower hotline that was accessible to both external individuals and employees within the Company.	No exceptions noted.
ELC-14	Management has established defined roles and responsibilities to oversee the implementation of the security and control environment.	Inspected the information security policy to determine that management had established defined roles and responsibilities to oversee the implementation of the security and control environment.	No exceptions noted.
HALP-1	The Company maintains internal informational websites describing the system environment, its boundaries, user responsibilities, and services. Halp maintains an architecture page to communicate how the Halp application is composed.	Inspected the Atlassian intranet to determine that the Company maintained internal information websites describing the system environment, its boundaries, user responsibilities, and services.	No exceptions noted.
		Inspected the Halp Architecture page to determine that Halp maintained an architecture page to communicate how the Halp application was composed.	No exceptions noted.

Communication and Information			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
HR-1	The hiring manager reviews and approves job descriptions.	Inspected job descriptions for a sample of employees supporting the service to determine that job descriptions were documented, reviewed, and approved by the hiring manager, and included authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	No exceptions noted.
HR-9	User awareness training is performed at least annually for employees and contractors as part of the Atlassian Security Awareness program.	Inspected training completion evidence for a sample of employees and contractors to determine that user awareness training was performed at least annually as part of the Atlassian Security Awareness program.	Exception noted. For 3 of 44 employees and contractors sampled, user awareness training was not completed during the period.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.		
CMC-1	Significant changes made to the system are communicated to customers via the Atlassian customer facing website.	Inspected the Atlassian website to determine significant changes to the system are communicated to customers through the customer facing website.	No exceptions noted.
CMC-3	Terms of service (ToS) are standardized and approved by legal. The Atlassian Trust Security page and ToS communicates Atlassian's commitments and the customer responsibilities. The Atlassian Trust Security page and ToS are published on the Atlassian customer facing website and any changes are communicated.	Inspected the Atlassian Trust Security page and ToS to determine that the Company's commitments were communicated to customers.	No exceptions noted.
		Inspected the customer facing website to determine that the Atlassian Trust Security page and ToS were published and any changes to the Atlassian Trust Security page or ToS were communicated.	No exceptions noted.

Communication and Information			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CMC-4	Atlassian communicates changes to confidentiality commitments to its customers, vendors, and internal users through the Atlassian website, when applicable.	Inspected the Atlassian website to determine that Atlassian communicated changes to confidentiality commitments during the period to its customers, vendors, and internal users through the Atlassian website, when applicable	No exceptions noted.
HALP-5	Descriptions of the system and its boundaries are available to external users via ongoing communications with customers, in official blog posts, and through the Statuspage website.	Inspected the external-facing website to determine that descriptions of the system and its boundaries were available to external users via ongoing communications with customers, in official blog posts, and through the Statuspage website.	No exceptions noted.
HALP-6	Availability is published so that customers may check the status and uptime of Halp.	Inspected the external-facing website to determine that availability was published so that customers could check the status and uptime of Halp.	No exceptions noted.
VDR-1	Vendor agreements include security, availability, and confidentiality commitments, and are reviewed during the procurement process.	Inspected contracts for a sample of critical vendors to determine that formal information sharing agreements were reviewed during the procurement process and included any applicable security, availability, and confidentiality commitments.	No exceptions noted.

Risk Assessment			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.		
RM-1	The Atlassian Risk and Compliance team evaluates the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Atlassian maintains a risk and controls matrix within the GRC Tool.	Inspected the Atlassian GRC Tool to determine that the Atlassian Risk and Compliance team evaluated the design of controls and mitigation strategies during the period, including identifying risks and recommending changes in the control environment.	No exceptions noted.
		Inspected the Atlassian GRC Tool to determine that Atlassian maintained a risk and controls matrix within their GRC Tool.	No exception noted.
RM-2	Atlassian has defined an ERM process and conducts an enterprise risk assessment on an annual basis, which includes key product stakeholders.	Inspected the Enterprise Risk Management Program to determine that Atlassian has defined an ERM process.	No exceptions noted.
		Inspected risk assessment documentation to determine that an enterprise risk assessment occurred during the period and included key product stakeholders.	No exceptions noted.

Risk Assessment			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.		
RM-2	Atlassian has defined an ERM process and conducts an enterprise risk assessment on an annual basis, which includes key product stakeholders.	Inspected the Enterprise Risk Management Program to determine that Atlassian has defined an ERM process.	No exceptions noted.
		Inspected risk assessment documentation to determine that an enterprise risk assessment occurred during the period and included key product stakeholders.	No exceptions noted.
RM-3	A fraud risk assessment is performed annually by the Head of Risk and Compliance. A cross-functional survey of employees in areas susceptible to fraud is conducted and combined with an evaluation of external risks. Results are evaluated by the Head of Risk and Compliance. The results are included with the enterprise risk assessment.	Inspected fraud risk assessment documentation to determine that a fraud risk assessment was performed by the Head of Risk and Compliance during the period and results were included as a part of the enterprise risk assessment.	No exceptions noted.
		Inspected fraud risk assessment documentation to determine that a cross-functional survey of employees in areas susceptible to fraud was conducted and combined with an evaluation of external risks and that results were evaluated by the Head of Risk and Compliance	No exceptions noted.

Risk Assessment			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.		
RM-2	Atlassian has defined an ERM process and conducts an enterprise risk assessment on an annual basis, which includes key product stakeholders.	Inspected the Enterprise Risk Management Program to determine that Atlassian has defined an ERM process.	No exceptions noted.
		Inspected risk assessment documentation to determine that an enterprise risk assessment occurred during the period and included key product stakeholders.	No exceptions noted.
RM-3	A fraud risk assessment is performed annually by the Head of Risk and Compliance. A cross-functional survey of employees in areas susceptible to fraud is conducted and combined with an evaluation of external risks. Results are evaluated by the Head of Risk and Compliance. The results are included with the enterprise risk assessment.	Inspected fraud risk assessment documentation to determine that a fraud risk assessment was performed by the Head of Risk and Compliance during the period and results were included as a part of the enterprise risk assessment.	No exceptions noted.
		Inspected fraud risk assessment documentation to determine that a cross-functional survey of employees in areas susceptible to fraud was conducted and combined with an evaluation of external risks and that results were evaluated by the Head of Risk and Compliance	No exceptions noted.

Risk Assessment			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.		
MTR-3	Penetration testing is performed by a bug bounty program on a continuous basis. Vulnerabilities are reviewed, prioritized, and resolved within the defined time frame.	Inspected the penetration test report from the bug bounty program for the period to determine that penetration testing was performed during the period, by a bug bounty program on a continuous basis.	No exceptions noted.
		Inspected Jira tickets for a sample of vulnerabilities to determine that vulnerabilities were reviewed, prioritized, and resolved within the defined time frame.	No exceptions noted.
RM-2	Atlassian has defined an ERM process and conducts an enterprise risk assessment on an annual basis, which includes key product stakeholders.	Inspected the Enterprise Risk Management Program to determine that Atlassian has defined an ERM process.	No exceptions noted.
		Inspected risk assessment documentation to determine that an enterprise risk assessment occurred during the period and included key product stakeholders.	No exceptions noted.

Risk Assessment			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
RM-3	A fraud risk assessment is performed annually by the Head of Risk and Compliance. A cross-functional survey of employees in areas susceptible to fraud is conducted and combined with an evaluation of external risks. Results are evaluated by the Head of Risk and Compliance. The results are included with the enterprise risk assessment.	Inspected fraud risk assessment documentation to determine that a fraud risk assessment was performed by the Head of Risk and Compliance during the period and results were included as a part of the enterprise risk assessment.	No exceptions noted.
		Inspected fraud risk assessment documentation to determine that a cross-functional survey of employees in areas susceptible to fraud was conducted and combined with an evaluation of external risks and that results were evaluated by the Head of Risk and Compliance	No exceptions noted.

Monitoring Activities			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.		
MTR-2	Continuous internal and external network vulnerability scanning is performed over the Atlassian environment. Vulnerabilities are reviewed, prioritized, and resolved as per the defined time frame.	Inspected continuous internal and external network vulnerability scan configurations to determine that internal and external network vulnerability scans were performed continuously to identify, quantify, and prioritize vulnerabilities.	No exceptions noted.
		Inspected remediation documentation for a sample of vulnerabilities identified during the period to determine vulnerabilities were resolved within Atlassian's standard resolution time frames.	No exceptions noted.
MTR-3	Penetration testing is performed by a bug bounty program on a continuous basis. Vulnerabilities are reviewed, prioritized, and resolved within the defined time frame.	Inspected the penetration test report from the bug bounty program for the period to determine that penetration testing was performed during the period, by a bug bounty program on a continuous basis.	No exceptions noted.
		Inspected Jira tickets for a sample of vulnerabilities to determine that vulnerabilities were reviewed, prioritized, and resolved within the defined time frame.	No exceptions noted.
RM-4	Internal audits are performed annually and results are communicated to management and the Audit Committee. Corrective actions are monitored.	Inspected internal audit documentation and test results to determine that internal audits were performed during the period and that the results were communicated to management and the Audit Committee, and corrective actions were monitored.	No exceptions noted.

Monitoring Activities			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
VDR-2	Atlassian reviews the SOC reports of its vendors on an annual basis.	Inspected SOC report review documentation for a sample of vendors to determine that SOC report reviews were performed during the period.	No exceptions noted.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.		
RM-4	Internal audits are performed annually and results are communicated to management and the Audit Committee. Corrective actions are monitored.	Inspected internal audit documentation and test results to determine that internal audits were performed during the period and that the results were communicated to management and the Audit Committee, and corrective actions were monitored.	No exceptions noted.
VDR-2	Atlassian reviews the SOC reports of its vendors on an annual basis.	Inspected SOC report review documentation for a sample of vendors to determine that SOC report reviews were performed during the period.	No exceptions noted.

Control Activities			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.		
RM-1	The Atlassian Risk and Compliance team evaluates the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Atlassian maintains a risk and controls matrix within the GRC Tool.	Inspected the Atlassian GRC Tool to determine that the Atlassian Risk and Compliance team evaluated the design of controls and mitigation strategies during the period, including identifying risks and recommending changes in the control environment.	No exceptions noted.
		Inspected the Atlassian GRC Tool to determine that Atlassian maintained a risk and controls matrix within their GRC Tool.	No exceptions noted.
RM-2	Atlassian has defined an ERM process and conducts an enterprise risk assessment on an annual basis, which includes key product stakeholders.	Inspected the Enterprise Risk Management Program to determine that Atlassian has defined an ERM process.	No exceptions noted.
		Inspected risk assessment documentation to determine that an enterprise risk assessment occurred during the period and included key product stakeholders.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.		
RM-1	The Atlassian Risk and Compliance team evaluates the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Atlassian maintains a risk and controls matrix within the GRC Tool.	Inspected the Atlassian GRC Tool to determine that the Atlassian Risk and Compliance team evaluated the design of controls and mitigation strategies during the period, including identifying risks and recommending changes in the control environment.	No exceptions noted.

Control Activities			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected the Atlassian GRC Tool to determine that Atlassian maintained a risk and controls matrix within their GRC Tool.	No exceptions noted.
RM-2	Atlassian has defined an ERM process and conducts an enterprise risk assessment on an annual basis, which includes key product stakeholders.	Inspected the Enterprise Risk Management Program to determine that Atlassian has defined an ERM process.	No exceptions noted.
		Inspected risk assessment documentation to determine that an enterprise risk assessment occurred during the period and included key product stakeholders.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.		
CHG-12	A formal systems development life cycle (SDLC) methodology is in place that governs the development, acquisition, implementation, changes, and maintenance of information systems and related technology requirements.	Inspected SDLC documentation to determine that an SDLC methodology was in place that governed the development, acquisition, implementation, changes, and maintenance of information systems and related technology requirements.	No exceptions noted.
DS-2	An Information Classification Policy is in place to support the safety and security of Atlassian's data.	Inspected the Information Classification Policy to determine that a data classification policy was in place to support the safety and security of Atlassian's data.	No exceptions noted.
ELC-3	Policies are posted and available, assigned a policy owner, and reviewed at least annually.	Inspected the Atlassian intranet to determine that policies were posted and available online, assigned a policy owner, and were reviewed during the period.	No exceptions noted.

Control Activities			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
ELC-15	Formal procedures are documented that outline the process the Company's staff follows to perform the following system access control functions: - Adding new users - Modifying an existing user's access - Removing an existing user's access - Restricting access based on separation of duties and least privilege	Inspected system access control procedures to determine that formal procedures were documented that outlined the process the Company's staff followed to perform the following system access control functions: - Adding new users - Modifying an existing user's access - Removing an existing user's access - Restricting access based on separation of duties and least privilege	No exceptions noted.
ELC-16	Information security policies and procedures are documented and define the information security rules and requirements for the service environment.	Inspected the Company's information security policies and procedures to determine that they were documented and defined the information security rules and requirements for the service environment.	No exceptions noted.
ELC-17	Formal procedures are documented that outline the process the Company's staff follows to back up and recover customer data.	Inspected backup and recovery procedures to determine that formal procedures were documented that outlined the process the Company's staff followed to back up and recover customer data.	No exceptions noted.
ELC-18	Formal procedures are documented that outline requirements for vulnerability management and system monitoring. The procedures are reviewed at least annually.	Inspected formal vulnerability management and system monitoring procedures to determine that they were documented, were reviewed during the period, and outlined the requirements for vulnerability management and system monitoring.	No exceptions noted.

Control Activities			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
IM-1	An organizational wide incident management process is in place, with the SRE team responsible for incidents and problems for Atlassian services and platforms. Incident management processes must meet the Atlassian Incident Management Standard.	Inspected the Atlassian Incident Management Standard to determine an entity-wide process was in place and established responsibility for incidents and problems to the SRE team.	No exceptions noted.
		Inspected a sample of security events to determine security events and incidents were addressed in accordance with the Atlassian Incident Management Standard.	No exceptions noted.
RM-2	Atlassian has defined an ERM process and conducts an enterprise risk assessment on an annual basis, which includes key product stakeholders.	Inspected the Enterprise Risk Management Program to determine that Atlassian has defined an ERM process.	No exceptions noted.
		Inspected risk assessment documentation to determine that an enterprise risk assessment occurred during the period and included key product stakeholders.	No exceptions noted.
VDR-3	A vendor management program is in place. Components of this program include: - Maintaining a list of critical vendors - Requirements for critical vendors to maintain their own security practices and procedures - Annually reviewing attestation reports for critical vendors or performing a vendor risk assessment	Inspected the vendor management policy to determine that a vendor management program was in place and components of this program included: - Maintaining a list of critical vendors - Requirements for critical vendors to maintain their own security practices and procedures - Annually reviewing attestation reports for critical vendors or performing a vendor risk assessment	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
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.		
DS-3	A ZeroTrust infrastructure is implemented to place endpoints into a tiered network (High, Trusted, Open) based on their security posture and type of device. Applications added to the SSO platform are tiered according to the ZeroTrust policy. Endpoints cannot access applications via the SSO platform unless they are placed on the same/higher tier as the application.	Inspected the ZeroTrust Service Tier Standard and the Endpoint Minimum Baseline Configuration Standard and observed applications on the SSO platform to determine that a ZeroTrust infrastructure was implemented to place endpoints into a tiered network (High, Trusted, Open) based on their security posture and type of device.	No exceptions noted.
		Inspected the ZeroTrust Service Tier Standards and the Endpoint Minimum Baseline Configuration Standard to determine that applications added to the SSO platform are tiered according to the ZeroTrust policy.	No exceptions noted.
		Observed an endpoint without required configurations and tier placement per the Endpoint Minimum Baseline Configuration Standard to determine that endpoints could not access applications via the SSO platform unless they were placed on the same/higher tier as the application.	No exceptions noted.
HALP-4	Halp assigns unique identifiers to customer accounts and uses the identifier to logically segregate customer data.	Inspected the database and customer account configurations to determine that Halp assigned unique identifiers to customer accounts and used the identifier to logically segregate customer data.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
HALP-16	Encryption is enabled for Halp customer data.	Inspected datastore configurations to determine that Halp customer data was configured to be encrypted at rest.	No exceptions noted.
IAM-1	Two-factor authentication is required when logging into VPN (Remote Access Service) from any IP address.	Inspected system configurations and observed a remote login session to determine that two-factor authentication was required when logging into VPN (Remote Access Service) from any IP address.	No exceptions noted.
IAM-5	Active Directory enforces password settings in line with the Atlassian Password Standard. Idaptive Single Sign On allows users to have a single point of authentication to access multiple applications. Passwords settings for Idaptive are enforced by Active Directory (AD) via the AD connector for Idaptive.	Inspected Active Directory password configurations and the Atlassian Password Standard to determine that Active Directory enforces password settings in line with the Atlassian Password Standard.	No exceptions noted.
		Inspected the Idaptive system configurations to determine that Idaptive Single Sign On allowed users to have a single point of authentication to access multiple applications and that passwords settings for Idaptive were enforced by AD via the AD connector for Idaptive.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.		
HALP-3	Access to customer data by the Halp Support team is supported by a valid customer support request.	Inspected system configurations to determine that access to customer data by the Halp Support team was supported by a valid customer support request.	Exception noted. Atlassian Internal Audit identified that a customer support's access to customer data was not configured to expire.
HALP-10	User access is approved by management prior to provisioning access.	Inspected the Halp access provisioning logs to determine that user access was approved by management prior to provisioning access.	No exceptions noted.
HALP-11	User profile and access reviews are performed semi-annually and include active user accounts for employees and contractors. Access issues, if any, are investigated and resolved.	Inspected access review documentation for a sampled review to determine that user profile and access reviews were performed semi-annually and included active user accounts for employees and contractors.	No exceptions noted.
		Inspected change tickets for a sample of changes that resulted from the access reviews to determine that access issues, if any, were investigated and resolved.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
IAM-3	Access to the Atlassian internal network and internal tools is restricted to authorized users via logical access measures: • Each Atlassian user must have an active Active Directory account. • Each Atlassian user must be members of the appropriate LDAP group.	Inspected system configurations and observed logins to the Atlassian internal network and tools to determine that access to the Atlassian internal network and internal tools was restricted to authorized users via logical access measures: • Each Atlassian user must have an active Active Directory account. • Each Atlassian user must be members of the appropriate LDAP group.	No exceptions noted.
IAM-4	Active Directory group membership is automatically assigned based on the user's department and team.	Inspected system configurations to determine that Active Directory group membership was automatically assigned based on the user's department and team.	No exceptions noted.
IAM-6	An automatic alert is triggered to the WPT or HR Information Systems Manager for any role change between the following groups: Engineering, Customer Support & Success (CSS), and Finance. Appropriateness of access is reviewed and approved.	Inspected alert threshold configurations and example alerts to determine that automatic alerts were triggered to the WPT or HR Information Systems Manager for any role change between the following groups: Engineering, CSS, and Finance.	No exceptions noted.
		Inspected access review and approval documentation for a sample of alerts to determine that appropriateness of access was reviewed and approved.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
IAM-7	Active directory accounts and network access are automatically disabled within 8 hours from the time an employee is marked as terminated in the HR system.	Inspected Idaptive system configurations to determine that active directory accounts and network access was set to be automatically disabled within 8 hours from the time an employee was marked as terminated in the HR system.	No exceptions noted.
IAM-8	The HR system does not allow terminations to be backdated.	Observed a demonstration of the HR system to determine that the HR system did not allow terminations to be backdated.	No exceptions noted.
IAM-9	On a semi-annual basis, the Build Engineering Development Team Lead performs a review of privileged user access for the authorized build system.	Inspected access review documentation for a sampled privileged user access review and ascertained that the Build Engineering Development Team Lead performed a review of privileged user access for authorized build system semi-annually.	No exceptions noted.
		Inspected change tickets for a sample of changes that resulted from the privileged access review to determine that change tickets were created to track access removals or modifications resulting from the review.	No exceptions noted.
IAM-10	On a semi-annual basis, the Active Directory and Idaptive system owner performs a user access review of privileged Active Directory and Idaptive access (including generic accounts) and Active Directory Admin Accounts.	Inspected access review documentation for a sampled access review to determine that the Active Directory and Idaptive system owner performed a user access review of privileged Active Directory and Idaptive access (including generic accounts) and Active Directory Admin Accounts semi-annually.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected change tickets for a sample of changes that resulted from the privileged access review to determine that change tickets were created to track access removals or modifications resulting from the review.	No exceptions noted.
IAM-11	The People Central Systems Support Specialist performs a review over Workday admin users semi-annually.	Inspected access review documentation for a sampled review to determine that the People Central Systems Support Specialist performed a review over Workday admin users semi-annually.	No exceptions noted.
IAM-12	Access to critical systems and services the Bitbucket Pipelines team uses to administer the service is reviewed semi-annually.	Inspected access review documentation for a sampled review to determine that access to critical systems and services the Bitbucket Pipelines team used to administer the service were reviewed semi-annually.	No exceptions noted.
IAM-14	The Build Engineering team performs a semi-annual access review for Artifactory.	Inspected access review documentation for a sampled review to determine that the Build Engineering team performed a semi-annual access review for Artifactory.	No exceptions noted.
MICROS-6	Atlassian's Engineering Managers or Team Leads perform a user access review over the Micros Platform and the associated in-scope supporting databases, tools, and services semi-annually.	Inspected access review documentation for a sampled review to determine that Atlassian's Engineering Managers or Team Leads performed a user access review over the Micros Platform and the associated in-scope supporting databases, tools, and services semi-annually.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.		
HALP-9	Administrator access is restricted to authorized system and security administrators.	Inspected privileged user access to the Halp and the users' job role for in-scope systems to determine that administrator access was restricted to authorized system and security administrators.	No exceptions noted.
IAM-7	Active directory accounts and network access are automatically disabled within 8 hours from the time an employee is marked as terminated in the HR system.	Inspected Idaptive system configurations to determine that active directory accounts and network access was set to automatically disabled within 8 hours from the time an employee was marked as terminated in the HR system.	No exceptions noted.
IAM-9	On a semi-annual basis, the Build Engineering Development Team Lead performs a review of privileged user access for the authorized build system.	Inspected access review documentation for a sampled privileged user access review and ascertained that the Build Engineering Development Team Lead performed a review of privileged user access for authorized build system semi-annually.	No exceptions noted.
		Inspected change tickets for a sample of changes that resulted from the privileged access review to determine that change tickets were created to track access removals or modifications resulting from the review.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
IAM-16	Micros will only pull deployment artifacts from the restricted namespace. Only privileged users of the authorized build system have the credentials to push to the restricted namespace.	Inspected system configurations to determine that Micros will only pull deployment artifacts from the restricted namespace.	No exceptions noted.
		Inspected system access listings, inquired of management, and compared each users' level of access to their job role to determine that only privileged users of the authorized build system had the credentials to push to the restricted namespace.	No exceptions noted.
IAM-17	User access is approved by management prior to provisioning access.	Inspected the Halp access provisioning logs to determine that user access was approved by management prior to provisioning access.	No exceptions noted.
MICROS-4	Privileged access of Atlassian users to the EC2 production environment is restricted to authorized and appropriate users only.	Inspected privileged access listings and the users' job role to determine that privileged access of Atlassian users to EC2 production environment was restricted to authorized and appropriate users only.	No exceptions noted.
MICROS-5	Access to the AWS production environment, RDS databases, and supporting tools is provisioned via a documented approval in a Jira ticket or based on appropriate authorization by the service owner or delegate.	Inspected the access log for a sample of access changes to determine that access to the AWS production environment, RDS databases, and supporting tools was provisioned based on appropriate authorization by the service owner or delegate.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.		
INV-1	The Company's production environment is hosted at third-party data centers, which are carved out for the purposes of this report.	Not applicable.	Not applicable.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.		
INV-1	A formal inventory of production system assets that includes asset owners is maintained, and changes to the inventory are logged.	Inspected the production system asset inventory to determine that a formal inventory of production system assets that included asset owners was maintained and changes to the inventory were logged.	No exceptions noted.
INV-2	Electronic media containing confidential information is purged or destroyed, and evidence of the purging or destruction is retained for each device destroyed.	Inspected evidence of electronic media purging or destruction for a sample of purged or destroyed media to determine that electronic media containing confidential information was purged or destroyed and evidence of the purging or destruction was retained for each device destroyed.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
HALP-15	Remote connections and data in transit over public networks are encrypted using encryption protocols such as SSH or TLS 1.2.	Inspected transmission protocol configurations to determine that remote connections and data in transit over public networks were encrypted using encryption protocols such as SSH or TLS 1.2.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
IAM-1	Two-factor authentication is required when logging into VPN (Remote Access Service) from any IP address.	Inspected system configurations and observed a remote login session to determine that two-factor authentication was required when logging into VPN (Remote Access Service) from any IP address.	No exceptions noted.
IAM-2	Two-factor authentication is required when launching an application from the single sign on system (Idaptive).	Inspected system configurations and observed a remote login session to determine that two-factor authentication was required when launching an application from the single sign on system (Idaptive).	No exceptions noted.
MICROS-3	Direct access to the Micros Platform via JumpBox requires a valid SSH key and two factor authentication.	Observed a remote login session to determine that direct access to the Micros Platform via JumpBox required a valid SSH key and two factor authentication.	No exceptions noted.
MICROS-8	Firewall rules are in place and are configured using security policy rules to limit unnecessary ports, protocols, and services and are maintained by the Micros team. All changes to firewall rules require a peer reviewed pull request.	Inspected firewall configurations to determine that firewall rules were in place and were configured using security policy rules to limit unnecessary ports, protocols, and services and were maintained by the Micros team.	No exceptions noted.
		Inspected Bitbucket configurations to determine that all changes to firewall rules required a peer reviewed pull request.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
MTR-4	IT asset management software is used to enforce hard drive encryption, user authentication requirements, and security patching on MacOS endpoints.	Inspected the IT asset management software configurations to determine that IT asset management software was used to enforce hard drive encryption, user authentication requirements, and security patching on MacOS endpoints.	No exceptions noted.
MTR-5	IT Asset management software is used to monitor hard drive encryption, user authentication requirements, and security patching on Windows endpoints.	Inspected the IT asset management software configurations to determine that IT asset management software was used to monitor the hard drive encryption, user authentication requirements, and security patching was enforced on Windows endpoints.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.		
HALP-15	Remote connections and data in transit over public networks are encrypted using encryption protocols such as SSH or TLS 1.2.	Inspected transmission protocol configurations to determine that remote connections and data in transit over public networks were encrypted using encryption protocols such as SSH or TLS 1.2.	No exceptions noted.
MTR-4	IT asset management software is used to enforce hard drive encryption, user authentication requirements, and security patching on MacOS endpoints.	Inspected the IT asset management software configurations to determine that IT asset management software was used to enforce hard drive encryption, user authentication requirements, and security patching on MacOS endpoints.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
MTR-5	IT Asset management software is used to monitor hard drive encryption, user authentication requirements, and security patching on Windows endpoints.	Inspected the IT asset management software configurations to determine that IT asset management software was used to monitor the hard drive encryption, user authentication requirements, and security patching was enforced on Windows endpoints.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.		
MTR-1	Atlassian uses malware protection for Windows and OSX clients. An enterprise anti-malware platform provides endpoint protection, centralized reporting, and notifications. The client is installed via management platforms and protected by a complex password to prevent staff from removing or uninstalling the agent.	Inspected anti-malware software configurations to determine that Atlassian used malware protection for Windows and OSX clients that provides endpoint protection, centralized reporting, and notifications.	No exceptions noted.
		Inspected the anti malware software configurations to determine that the anti malware client was installed via management platforms and was protected by a complex password to prevent staff from removing or uninstalling the agent.	No exceptions noted.
MTR-4	IT asset management software is used to enforce hard drive encryption, user authentication requirements, and security patching on MacOS endpoints.	Inspected the IT asset management software configurations to determine that IT asset management software was used to enforce hard drive encryption, user authentication requirements, and security patching on MacOS endpoints.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
MTR-5	IT Asset management software is used to monitor hard drive encryption, user authentication requirements, and security patching on Windows endpoints.	Inspected the IT asset management software configurations to determine that IT asset management software was used to monitor the hard drive encryption, user authentication requirements, and security patching was enforced on Windows endpoints.	No exceptions noted.

System Operations			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.		
MTR-2	Continuous internal and external network vulnerability scanning is performed over the Atlassian environment. Vulnerabilities are reviewed, prioritized, and resolved as per the defined time frame.	Inspected continuous internal and external network vulnerability scan configurations to determine that internal and external network vulnerability scans were performed continuously to identify, quantify, and prioritize vulnerabilities.	No exceptions noted.
		Inspected remediation documentation for a sample of vulnerabilities identified during the period to determine vulnerabilities were resolved within Atlassian's standard resolution time frames.	No exceptions noted.
MTR-4	IT asset management software is used to enforce hard drive encryption, user authentication requirements, and security patching on MacOS endpoints.	Inspected the IT asset management software configurations to determine that IT asset management software was used to enforce hard drive encryption, user authentication requirements, and security patching on MacOS endpoints.	No exceptions noted.
MTR-5	IT Asset management software is used to monitor hard drive encryption, user authentication requirements, and security patching on Windows endpoints.	Inspected the IT asset management software configurations to determine that IT asset management software was used to monitor the hard drive encryption, user authentication requirements, and security patching was enforced on Windows endpoints.	No exceptions noted.

System Operations			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
RM-2	Atlassian has defined an ERM process and conducts an enterprise risk assessment on an annual basis, which includes key product stakeholders.	Inspected the Enterprise Risk Management Program to determine that Atlassian has defined an ERM process.	No exceptions noted.
		Inspected risk assessment documentation to determine that an enterprise risk assessment occurred during the period and included key product stakeholders.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.		
MTR-2	Continuous internal and external network vulnerability scanning is performed over the Atlassian environment. Vulnerabilities are reviewed, prioritized, and resolved as per the defined time frame.	Inspected continuous internal and external network vulnerability scan configurations to determine that internal and external network vulnerability scans were performed continuously to identify, quantify, and prioritize vulnerabilities.	No exceptions noted.
		Inspected remediation documentation for a sample of vulnerabilities identified during the period to determine vulnerabilities were resolved within Atlassian's standard resolution time frames.	No exceptions noted.

System Operations			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
MTR-3	Penetration testing is performed by a bug bounty program on a continuous basis. Vulnerabilities are reviewed, prioritized, and resolved within the defined time frame.	Inspected the penetration test report from the bug bounty program for the period to determine that penetration testing was performed during the period, by a bug bounty program on a continuous basis.	No exceptions noted.
		Inspected Jira tickets for a sample of vulnerabilities to determine that vulnerabilities were reviewed, prioritized, and resolved within the defined time frame.	No exceptions noted.
MTR-6	A log management tool is utilized to identify trends that may have a potential impact on the Company's ability to achieve its security objectives and generates alerts when specific events occur.	Inspected the log management tool configurations to determine that a log management tool was utilized to identify trends that may have had a potential impact on the Company's ability to achieve its security objectives and generated alerts when specific events occurred.	No exceptions noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.		
IM-1	An organizational wide incident management process is in place, with the SRE team responsible for incidents and problems for Atlassian services and platforms. Incident management processes must meet the Atlassian Incident Management Standard.	Inspected the Atlassian Incident Management Standard to determine an entity-wide process was in place and established responsibility for incidents and problems to the SRE team.	No exceptions noted.
		Inspected a sample of security events to determine security events and incidents were addressed in accordance with the Atlassian Incident Management Standard.	No exceptions noted.

System Operations			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
MTR-2	Continuous internal and external network vulnerability scanning is performed over the Atlassian environment. Vulnerabilities are reviewed, prioritized, and resolved as per the defined time frame.	Inspected continuous internal and external network vulnerability scan configurations to determine that internal and external network vulnerability scans were performed continuously to identify, quantify, and prioritize vulnerabilities.	No exceptions noted.
		Inspected remediation documentation for a sample of vulnerabilities identified during the period to determine vulnerabilities were resolved within Atlassian's standard resolution time frames.	No exceptions noted.
MTR-3	Penetration testing is performed by a bug bounty program on a continuous basis. Vulnerabilities are reviewed, prioritized, and resolved within the defined time frame.	Inspected the penetration test report from the bug bounty program for the period to determine that penetration testing was performed during the period, by a bug bounty program on a continuous basis.	No exceptions noted.
		Inspected Jira tickets for a sample of vulnerabilities to determine that vulnerabilities were reviewed, prioritized, and resolved within the defined time frame.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.		
HALP-17	Monitoring and alarming are configured to identify and notify management of incidents when thresholds are crossed on key security and operational metrics. Issues are resolved in accordance with incident management processes.	Inspecting availability and processing capacity monitoring tool configurations to determine that monitoring and alarming were configured to identify and notify management of incidents when thresholds were crossed on key security and operational metrics.	No exceptions noted.

System Operations			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected a sample of availability and processing capacity monitoring alerts to determine that issues were resolved in accordance with incident management processes.	No exceptions noted.
IM-1	An organizational wide incident management process is in place, with the SRE team responsible for incidents and problems for Atlassian services and platforms. Incident management processes must meet the Atlassian Incident Management Standard.	Inspected the Atlassian Incident Management Standard to determine an entity-wide process was in place and established responsibility for incidents and problems to the SRE team.	No exceptions noted.
		Inspected a sample of security events to determine security events and incidents were addressed in accordance with the Atlassian Incident Management Standard.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.		
DR-1	A disaster recovery policy is in place and is reviewed on an annual basis by the disaster recovery steering committee.	Inspected the disaster recovery policy and review documentation to determine that a disaster recovery policy is in place and was reviewed during the period by the disaster recovery steering committee.	No exceptions noted.
HALP-14	A formal disaster recovery plan is in place for Halp and is tested quarterly.	Inspected the Halp disaster recovery plan to determine that a formal disaster recovery plan was in place for Halp.	No exceptions noted.
		Inspected disaster recovery plan testing to determine that the Halp disaster recovery plan was tested quarterly.	No exceptions noted.

System Operations			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
IM-1	An organizational wide incident management process is in place, with the SRE team responsible for incidents and problems for Atlassian services and platforms. Incident management processes must meet the Atlassian Incident Management Standard.	Inspected the Atlassian Incident Management Standard to determine an entity-wide process was in place and established responsibility for incidents and problems to the SRE team.	No exceptions noted.
		Inspected a sample of security events to determine security events and incidents were addressed in accordance with the Atlassian Incident Management Standard.	No exceptions noted.

Change Management			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
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.		
CHG-2	Bitbucket does not allow a pull request to be approved by the same user who requests it.	Inspected system configurations to determine that Bitbucket did not allow a pull request to be approved by the same user who requested it.	No exceptions noted.
CHG-5	A Jira ticket is automatically generated if a change to the enforcement of peer review occurs.	Inspected system configurations to determine that a Jira ticket was automatically generated if a change to the enforcement of peer review occurs.	No exceptions noted.
CHG-6	Tokenator performs a check when building code designed for deployment to the SOX namespace on Micros to validate that the Bitbucket Cloud "Compliance" setting is enforced on the branch that the build is occurring from.	Inspected system configurations to determine that Tokenator performed a check when building code designed for deployment to the SOX namespace on Micros to validate that the Bitbucket Cloud "Compliance" setting was enforced on the branch that the build was occurring from.	No exceptions noted.
CHG-9	Changes to Bitbucket Pipelines must be peer reviewed prior to production deployment.	Inspected the system configurations to determine that changes to Bitbucket Pipelines must be peer reviewed prior to production deployment	No exceptions noted.
CHG-10	Bitbucket Pipelines will not allow code to be deployed unless it has passed green build testing.	Inspected the system configurations to determine that Bitbucket Pipelines will not allow code to be deployed unless it has passed green build testing.	No exceptions noted.
CHG-11	Write access to production software artifacts in Artifactory is limited to the Build Engineering team, the authorized build system, and the Micros server.	Inspected access listings and user job roles to determine that write access to production software artifacts in Artifactory was limited to the Build Engineering team, the authorized build system, and the Micros server.	No exceptions noted.

Change Management			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
HALP-7	Change control, as defined by policy, requires approval and a peer review prior to implementation.	Inspected the code repository configurations to determine that change control required approval and a peer review prior to implementation.	No exceptions noted.
HALP-8	Changes are tested according to the nature of the change in an environment separate from production prior to deployment into a production release.	Inspected the code repository configurations to determine that changes were tested according to the nature of the change in an environment separate from production prior to deployment into a production release.	No exceptions noted.
MICROS-2	Micros will only pull deployment artifacts from the restricted namespace. Only privileged users of the authorized build system have the credentials to push to the restricted namespace.	Inspected system configurations to determine that Micros will only pull deployment artifacts from the restricted namespace.	No exceptions noted.
		Inspected system access listings, inquired of management, and compared each users' level of access to their job role to determine that only privileged users of the authorized build system had the credentials to push to the restricted namespace.	No exceptions noted.

Risk Mitigation			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.		
DR-1	A disaster recovery policy is in place and is reviewed on an annual basis by the disaster recovery steering committee.	Inspected the disaster recovery policy and review documentation to determine that a disaster recovery policy is in place and was reviewed during the period by the disaster recovery steering committee.	No exceptions noted.
HALP-12	Critical system components are replicated across multiple availability zones to permit the resumption of critical operations in the event of the loss of a critical facility.	Inspected replication configurations to determine that critical system components were replicated across multiple availability zones to permit the resumption of critical operations in the event of the loss of a critical facility.	No exceptions noted.
HALP-14	A formal disaster recovery plan is in place for Halp and is tested quarterly.	Inspected the Halp disaster recovery plan to determine that a formal disaster recovery plan was in place for Halp.	No exceptions noted.
		Inspected disaster recovery plan testing to determine that the Halp disaster recovery plan was tested quarterly.	No exceptions noted.
IM-1	An organizational wide incident management process is in place, with the SRE team responsible for incidents and problems for Atlassian services and platforms. Incident management processes must meet the Atlassian Incident Management Standard.	Inspected the Atlassian Incident Management Standard to determine an entity-wide process was in place and established responsibility for incidents and problems to the SRE team.	No exceptions noted.
		Inspected a sample of security events to determine security events and incidents were addressed in accordance with the Atlassian Incident Management Standard.	No exceptions noted.

Risk Mitigation			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
MICROS-7	Replication is in place to provide data redundancy and availability for Micros.	Inspected database configurations and example alerts to determine that databases were replicated to secondary availability zones in real time and alerts were configured to notify administrators if replication failed.	No exceptions noted.
RM-1	The Atlassian Risk and Compliance team evaluates the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Atlassian maintains a risk and controls matrix within the GRC Tool.	Inspected the Atlassian GRC Tool to determine that the Atlassian Risk and Compliance team evaluated the design of controls and mitigation strategies during the period, including identifying risks and recommending changes in the control environment.	No exceptions noted.
		Inspected the Atlassian GRC Tool to determine that Atlassian maintained a risk and controls matrix within their GRC Tool.	No exception noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.		
VDR-1	Vendor agreements include security, availability, and confidentiality commitments, and are reviewed during the procurement process.	Inspected contracts for a sample of critical vendors to determine that formal information sharing agreements were reviewed during the procurement process and included any applicable security, availability, and confidentiality commitments.	No exceptions noted.
VDR-2	Atlassian reviews the SOC reports of its vendors on an annual basis.	Inspected SOC report review documentation for a sample of vendors to determine that SOC report reviews were performed during the period.	No exceptions noted.

Additional Criteria for Availability

Availability			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.		
HALP-17	Monitoring and alarming are configured to identify and notify management of incidents when thresholds are crossed on key security and operational metrics. Issues are resolved in accordance with incident management processes.	Inspecting availability and processing capacity monitoring tool configurations to determine that monitoring and alarming were configured to identify and notify management of incidents when thresholds were crossed on key security and operational metrics.	No exceptions noted.
		Inspected a sample of availability and processing capacity monitoring alerts to determine that issues were resolved in accordance with incident management processes.	No exceptions noted.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.		
DR-1	A disaster recovery policy is in place and is reviewed on an annual basis by the disaster recovery steering committee.	Inspected the disaster recovery policy and review documentation to determine that a disaster recovery policy is in place and was reviewed during the period by the disaster recovery steering committee.	No exceptions noted.
ELC-17	Formal procedures are documented that outline the process the Company's staff follows to back up and recover customer data.	Inspected backup and recovery procedures to determine that formal procedures were documented that outlined the process the Company's staff followed to back up and recover customer data.	No exceptions noted.

Availability			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
HALP-12	Critical system components are replicated across multiple availability zones to permit the resumption of critical operations in the event of the loss of a critical facility.	Inspected replication configurations to determine that critical system components were replicated across multiple availability zones to permit the resumption of critical operations in the event of the loss of a critical facility.	No exceptions noted.
HALP-13	Backups of critical system components are performed hourly. Backup restoration tests are performed quarterly to verify the recoverability of data.	Inspected backup configurations to determine that backups of critical system components were performed hourly.	No exceptions noted.
		Inspected backup restoration test documentation for a sample of quarters to determine that backup restoration tests were performed quarterly to verify the recoverability of data.	No exceptions noted.
HALP-14	A formal disaster recovery plan is in place for Halp and is tested quarterly.	Inspected the Halp disaster recovery plan to determine that a formal disaster recovery plan was in place for Halp.	No exceptions noted.
		Inspected disaster recovery plan testing to determine that the Halp disaster recovery plan was tested quarterly.	No exceptions noted.
MICROS-7	Replication is in place to provide data redundancy and availability for Micros.	Inspected database configurations and example alerts to determine that databases were replicated to secondary availability zones in real time and alerts were configured to notify administrators if replication failed.	No exceptions noted.

Availability			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.		
DR-1	A disaster recovery policy is in place and is reviewed on an annual basis by the disaster recovery steering committee.	Inspected the disaster recovery policy and review documentation to determine that a disaster recovery policy is in place and was reviewed during the period by the disaster recovery steering committee.	No exceptions noted.
ELC-17	Formal procedures are documented that outline the process the Company's staff follows to back up and recover customer data.	Inspected backup and recovery procedures to determine that formal procedures were documented that outlined the process the Company's staff followed to back up and recover customer data.	No exceptions noted.
HALP-13	Backups of critical system components are performed hourly. Backup restoration tests are performed quarterly to verify the recoverability of data.	Inspected backup configurations to determine that backups of critical system components were performed hourly.	No exceptions noted.
		Inspected backup restoration test documentation for a sample of quarters to determine that backup restoration tests were performed quarterly to verify the recoverability of data.	No exceptions noted.
HALP-14	A formal disaster recovery plan is in place for Halp and is tested quarterly.	Inspected the Halp disaster recovery plan to determine that a formal disaster recovery plan was in place for Halp.	No exceptions noted.
		Inspected disaster recovery plan testing to determine that the Halp disaster recovery plan was tested quarterly.	No exceptions noted.

Additional Criteria for Confidentiality

Confidentiality			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.		
DS-1	Production data is not used in non-production environments and must be protected in alignment with Atlassian's System Acquisition, Development, and Maintenance Policy.	Inspected the System Acquisition, Development, and Maintenance policy to determine that production data was prohibited by policy from being used or stored in non-production systems or environments.	No exceptions noted.
		Observed the test environment to determine that production data was not used in non-production systems or environments and was protected in alignment with Atlassian's System Acquisition, Development, and Maintenance Policy.	No exceptions noted.
DS-2	An Information Classification Policy is in place to support the safety and security of Atlassian's data.	Inspected the Information Classification Policy to determine that a data classification policy was in place to support the safety and security of Atlassian's data.	No exceptions noted.
VDR-1	Vendor agreements include security, availability, and confidentiality commitments, and are reviewed during the procurement process.	Inspected contracts for a sample of critical vendors to determine that formal information sharing agreements were reviewed during the procurement process and included any applicable security, availability, and confidentiality commitments.	No exceptions noted.

Confidentiality			
TSC Reference and Control #	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.		
HALP-2	Customer data is deleted from Halp systems within a reasonable period of time upon customer request.	Inspected evidence of data removal for a sample of customer requests for deletion of their data to determine that customer data was deleted from Halp systems within a reasonable period of time upon customer request.	No exceptions noted.
INV-2	Electronic media containing confidential information is purged or destroyed, and evidence of the purging or destruction is retained for each device destroyed.	Inspected evidence of electronic media purging or destruction for a sample of purged or destroyed media to determine that electronic media containing confidential information was purged or destroyed and evidence of the purging or destruction was retained for each device destroyed.	No exceptions noted.

Section 5

Other Information Provided by Atlassian Corporation Plc That Is Not Covered by the Service Auditor's Report

Management's Response to Testing Exceptions

Service Organization's Controls	Results of Tests	Management's Response
User awareness training is performed at least annually for employees and contractors as part of the Atlassian Security Awareness program.	Exception noted. For 3 of 44 employees and contractors sampled, user awareness training was not completed during the period.	Atlassian has confirmed the 3 sampled employees have either completed security training or are no longer employed by Atlassian.
Access to customer data by the Halp Support team is supported by a valid customer support request.	Exception noted. Atlassian Internal Audit identified that a customer support's access to customer data was not configured to expire.	Atlassian has confirmed that Halp support team members will require access to customer data until the support request is resolved. Hence a pre-defined time period to revoke access will not apply. Additionally, all access to customer data by the support team is configured to alert the customer through impersonation tooling configuration, ensuring access is not gained without their knowledge. This issue was identified proactively by Atlassian's internal audit team who raise a risk exception and will continue to monitor the design of the control to ensure that a customer supports access to customer data is expired upon ticket resolution.