COALFIRE
CONTROLS

# Report on Atlassian Corporation Plc's Description of Its Atlassian Cloud Products and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security, Availability, and Confidentiality Throughout the Period October 1, 2022 to September 30, 2023

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

ATLASSIAN

Jira Cloud | Confluence Cloud | Bitbucket Cloud | Opsgenie | Forge | Atlas | Jira Service Management
Jira Align | Jira Product Discovery | Jira Work Management | Data Lake | Atlassian Analytics | Compass
Statuspage | Trello | Halp

# Table of Contents

## Section 1

Independent Service Auditor’s Report ... 3

## Section 2

Assertion of Atlassian Corporation Plc Management ... 8

## Section 3

Atlassian Corporation Plc’s Description of Its Atlassian Cloud Products Throughout the Period October 1, 2022 to September 30, 2023 ... 10

## Section 4

Trust Services Criteria, Related Controls and Tests of Controls Relevant to the Security, Availability, and Confidentiality Categories ... 37

## Section 5

Other Information Provided by Atlassian Corporation Plc That Is Not Covered by the Service Auditor’s Report ... 86

# 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 Atlassian Cloud Products Throughout the Period October 1, 2022 to September 30, 2023" (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 (With Revised Implementation Guidance—2022*) (2018 description criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period October 1, 2022 to September 30, 2023, 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 (With Revised Points of Focus—2022)* (2017 TSC).

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. 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 and database hosting 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 Atlassian Cloud Products made available to user entities during the period October 1, 2022 to September 30, 2023. 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 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.

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

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.

## 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 the Atlassian Cloud Products that were designed and implemented throughout the period October 1, 2022 to September 30, 2023, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period October 1, 2022 to September 30, 2023, 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, 2022 to September 30, 2023, 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 the Atlassian Cloud Products during some or all of the period October 1, 2022 to September 30, 2023, business partners of Atlassian subject to risks arising from interactions with the Atlassian Cloud Products, 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

Greenwood Village, Colorado
December 12, 2023

# Section 2

# Assertion of Atlassian Corporation Plc Management

ATLASSIAN

**Assertion of Atlassian Corporation Plc (“Atlassian”) Management**

We have prepared the accompanying description in Section 3 titled “Atlassian Corporation Plc’s Description of Its Atlassian Cloud Products Throughout the Period October 1, 2022 to September 30, 2023” (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 (With Revised Implementation Guidance—2022*) (2018 description criteria). The description is intended to provide report users with information about the Atlassian Cloud Products 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 (With Revised Points of Focus—2022)* (2017 TSC).

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 and database hosting 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 the Atlassian Cloud Products that were designed and implemented throughout the period October 1, 2022 to September 30, 2023, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period October 1, 2022 to September 30, 2023, 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, 2022 to September 30, 2023, 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.

Vikram Rao
Chief Trust Officer
Atlassian Corporation Plc

# Section 3

# Atlassian Corporation Plc's Description of Its Atlassian Cloud Products Throughout the Period October 1, 2022 to September 30, 2023

# Type of Services Provided

## Company Overview and Background

Atlassian Corporation Plc (“Atlassian” or “the Company”) was established in 2002 and had its initial public offering (IPO) in 2015. Atlassian has employees working remotely across various countries, with offices around the world including the United States (San Francisco, Mountain View, New York City, Austin, Boston), Australia (Sydney), Philippines (Manila), Japan (Yokohama), Netherlands (Amsterdam), Poland (Gdansk), Turkey (Ankara), and India (Bengaluru).

Atlassian's ultimate goal is to unleash the potential in every team. Its collaboration software helps teams organize, discuss, and complete shared work. 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 together. Atlassian provides a range of products and services including Atlas, Atlassian Analytics, Bitbucket Cloud (including Bitbucket Pipelines), Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud (including Automation for Jira), Jira Service Management (including Assets), Jira Product Discovery, Jira Work Management, Opsgenie, Statuspage, and Trello.

This report focuses on the key operating systems that constitute the products and services hosted on Amazon Web Services (AWS) for all in-scope systems as well as Microsoft Azure (Azure) for Jira Align for customers who elect that option, along with the supporting information technology (IT) infrastructure and business processes. It does not include on-premise versions such as Jira and Confluence Server and Data Center, service enhancements that are not explicitly defined, add-ons obtained from the marketplace, and open source downloadables added by customers to their instance.

## Overview of Products and Services

### Products

**Atlas**

Atlas is a teamwork directory that connects and enables teams to openly communicate and obtain the context they need for their work. It enables customers to get a consolidated view of project status and progress across a defined set of their projects.

**Bitbucket Cloud**

Bitbucket Cloud is more than just Git code management. It provides teams with a single place to plan projects, collaborate on code, and perform integration testing. Customers use Bitbucket Cloud to track version-controlled changes to their software projects. With Bitbucket Cloud, customers can collaborate on code using inline comments and pull requests, while also managing and sharing their Git repositories to build and ship software as a team.

**Compass**

Compass allows customers to navigate their distributed architecture, bringing together disconnected information about engineering output and the teams collaborating on it. Important information, such as ownership, component details (run books, repositories, etc.), and scorecards, enables customers to prioritize and focus on what matters in a central, searchable location. Rich, real-time activity updates can be pulled from components and their dependencies, providing data across all tools in the software development toolchain.

### Confluence Cloud

Confluence Cloud is designed for creating a wide range of content, including meeting notes, product requirements, marketing plans, and human resources policies. It facilitates the organization of documentation by grouping related pages together in a dedicated space that can be accessed by individuals or the entire organization allowing for collaboration. With its search, structured page trees, and page archival, Confluence Cloud ensures that content is readily available and up to date.

### Jira Align

Jira Align is a scaled agile management system that utilizes Agile at Scale frameworks, such as the Scaled Agile Framework (SAFe), to provide visibility, coordination, and management at the program, portfolio, and enterprise levels. Jira Align offers services to customers globally, primarily in the technology industry. It simplifies software at scale by bringing together the business and software development organizations onto a single platform. Customers depend on Jira Align to scale beyond the individual team level and enable strategic decision-making, such as development capacity optimization and investment decisions.

### Jira Cloud

Jira Cloud is a software development tool used by agile teams to plan, track, and release software. It includes the Jira Suite, which consists of Jira Software, Automation for Jira, Jira Product Discovery, and Jira Work Management.

### Jira Service Management

Jira Service Management (JSM) is an IT service management (ITSM) solution built on the Jira platform that enables teams to collaborate, allowing them to respond to business changes and provide better experiences for customers and employees. JSM incorporates the power of Opsgenie and Assets, enhancing its functionality.

### Jira Product Discovery

Jira Product Discovery is a collaborative tool that allows teams to organize and prioritize ideas, share product roadmaps, and connect business and technical teams, all within Jira.

### Jira Work Management

Jira Work Management offers a platform for business teams and their projects, designed to facilitate cross-team coordination and eliminate silos.

### Opsgenie

Opsgenie is an incident management platform for operating always-on services, empowering DevOps teams to plan for service disruptions and stay in control during incidents. Opsgenie centralizes alerts, notifies designated people, and enables them to collaborate and take action. Throughout the entire incident lifecycle, Opsgenie tracks all activity and provides actionable insights to improve productivity and drive continuous operational efficiencies.

### Statuspage

Statuspage is a tool for incident communication that customers use to communicate real-time status of their internal or external services and display relevant metrics to their users. It helps to reduce the number of support requests during an incident with proactive customer communication. Customers can manage their subscribers directly in Statuspage and send consistent messages through the channel of their choice, such as email, text message, or in-application message.

### Trello

Trello is a visual collaboration tool that creates a shared perspective on any project. With a layout of boards, lists, and cards, it enables teams to get a shared perspective on projects. Trello is available via web or dedicated applications across desktop and mobile platforms.

## Services

### Assets

Assets is a configuration management database (CMDB) used to manage any type of structured data such as hardware, software, people, facilities, compliance, customers, and contracts.

### Atlassian Analytics

Atlassian Analytics is a data visualization platform that enables customers to create queries and dashboards, using data from various sources. Atlassian Analytics is built on top of Atlassian Data Lake, which provides clean, modeled data across Atlassian products (e.g., Jira Cloud) and ensures up-to-date access to data. With collaboration and sharing features, Atlassian Analytics also enables teams to work together in the context that best suits their needs.

### Automation for Jira

Automation for Jira (A4J) is a tool that is used to automate regular tasks within Jira. For instance, customers can add rules to update fields when the workflow is in a certain state. A4J enables customers to add rules without the need for coding.

### Bitbucket Pipelines

Bitbucket Pipelines, a service within Bitbucket Cloud, provides an integrated continuous integration and continuous delivery (CI/CD). It allows for deployment of bug fixes, features, and configuration changes into production through automation of acceptance and integration testing.

### Data Lake

With multi-region availability for Jira customers, Data Lake is designed to enable the querying of Atlassian product data using business intelligence (BI) tools such as Tableau with available integration into Atlassian Analytics.

### Forge

Forge is a platform that enables customers, ecosystem partners, and third-party vendors to create applications that customize, extend, and integrate with Atlassian Cloud Products. Forge offers built-in security, Atlassian-hosted infrastructure, and user interface (UI) extensibility options. Additionally, it provides a streamlined DevOps experience with development, staging, and production environments. The platform reduces the barriers to entry for application developers by providing a set of services that enables applications to become operational.

### Halp

Halp is a conversational ticketing solution for modern IT and operations teams to assign, prioritize, manage, and report on requests from various platforms. Integrated with messaging platforms, Halp enables customers to handle internal requests from end-users in a more streamlined manner.

The system description in this section of the report details Atlassian Cloud Products described above. Any other Company services are not within the scope of this report. The accompanying description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at any subservice organizations (see below for further discussion of the subservice organizations).

# Principal Service Commitments and System Requirements

Atlassian designs its processes and procedures to align with the objectives of the Atlassian Cloud Products. These objectives are formulated according to the service commitments made by Atlassian to user entities; the laws and regulations governing the provision of the Systems; and the financial, operational, and compliance requirements that Atlassian has established for the Systems.

The commitments to user entities regarding security, availability, and confidentiality are documented and communicated through various channels, such as Cloud Terms of Services, Product-Specific Terms of Services, the sign-up page, Privacy Policy, and Atlassian Trust Center. The commitments to security, availability, and confidentiality include, but not limited to:

| Trust Services Category | Service Commitments |
|---|---|
| **Security** | **All Products:**<br>• Atlassian will implement and maintain physical, technical and administrative security measures designed to protect customer data from unauthorized access, destruction, use, modification, or disclosure.<br>• Atlassian will maintain a compliance program that includes independent third-party audits and certifications.<br>• Upon becoming aware of a security incident, Atlassian will notify customers without undue delay. |
| **Availability** | **All Products excluding Jira Align:**<br>• Atlassian will use commercially reasonable efforts to maintain the availability of the products.<br>**Jira Align:**<br>• Atlassian shall use commercially reasonable efforts to make Jira Align available at least 99.5% of the time during each calendar month during the term excluding excusable downtime. |
| **Confidentiality** | **All Products:**<br>• Atlassian will not disclose confidential information to any third party unless they have a business need to know, and will not use confidential information for any purpose other than providing the services.<br>• Upon termination of the services, Atlassian will delete or return customer data in accordance with the retention periods. |

Atlassian establishes operational requirements that support the achievement of its security, availability, and confidentiality commitments as well as relevant laws and regulations and other system requirements. These requirements are communicated through Atlassian's system policies and procedures, system design documentation, and contracts with customers. Atlassian's information security policies define an organization-wide approach to protecting systems and data. These policies include those related to the design and development of services, operation of the systems, management of internal business systems and networks, and employee hiring and training. Standard operating procedures have been documented for carrying out specific manual and automated processes required for the operation and development of the Atlassian Cloud Products.

# Atlassian System Components

The boundaries of the Atlassian Cloud Products refer to the aspects of the company's infrastructure, software, personnel, procedures, and data that are essential for providing its services and that directly contribute to the services offered to customers. The sections below provide a description of the components that directly support the services offered to customers. Any infrastructure, software, personnel, procedures, or data that provide support indirectly are not included.

# Infrastructure

Atlassian Cloud Products utilize AWS data centers and infrastructure as a service (IaaS). Atlassian administrators oversee virtual server and operating system configurations through distinct AWS accounts and configuration management processes.

Similarly, Azure provides platform as a service (PaaS) for Jira Align's Enterprise Assets Business Intelligence solution.

Forge is designed for third-party application development, separated from the platform itself. Code is executed on AWS Lambda, which is managed by AWS. Forge management code operates on Amazon Elastic Compute Cloud (EC2) servers, with dedicated accounts for development and production.

Services are deployed in various regions to ensure redundancy and fault tolerance, including:

**Infrastructure - Products**

| Product | AWS Region(s) | | | Azure Region(s) | |
|---|---|---|---|---|---|
| | US | EU | AP | US | EU |
| Atlas | ✓ | ✓ | ✓ | | |
| Bitbucket Cloud | ✓ | | | | |
| Compass | ✓ | ✓ | ✓ | | |
| Confluence Cloud | ✓ | ✓ | ✓ | | |
| Jira Align | ✓ | ✓ | ✓ | ✓ | ✓ |
| Jira Cloud | ✓ | ✓ | ✓ | | |
| Jira Service Management | ✓ | ✓ | ✓ | | |
| Jira Product Discovery | ✓ | ✓ | ✓ | | |
| Jira Work Management | ✓ | ✓ | ✓ | | |
| Opsgenie | ✓ | ✓ | | | |
| Statuspage | ✓ | ✓ | ✓ | | |
| Trello | ✓ | | | | |

| Infrastructure - Services | | | |
|---|---|---|---|
| Service | AWS Region(s) | | |
| | US | EU | AP |
| Assets | ✓ | ✓ | ✓ |
| Atlassian Analytics | ✓ | ✓ | ✓ |
| Automation for Jira | ✓ | ✓ | ✓ |
| Bitbucket Pipelines | ✓ | ✓ | ✓ |
| Data Lake | ✓ | ✓ | ✓ |
| Forge | ✓ | | |
| Halp | ✓ | | |

## Network

Atlassian has public ingress points in multiple AWS and Azure regions. These traffic manager clusters terminate public Transport Layer Security (TLS) and forward the requests to proxies hosted in AWS and Azure regions. All AWS and Azure hosted network traffic is inside the Atlassian Cloud Network and all traffic in and between AWS and Azure regions uses AWS transit gateway or Virtual Private Cloud (VPC) peering. Encryption in transit is implemented to protect user authentication information and the corresponding session transmitted over the Internet or other public networks to ensure that data reaches its intended destination.

Connections to services and products are protected using secure connectivity protocols. At all points, the network traffic is encrypted with TLS 1.2 or higher. Certificates have defined expiry dates that are notified and tracked internally so that they can be updated prior to their expiry.

Advanced Encryption Standard (AES)-256 is enabled to ensure encryption at rest within all data stores of Atlassian products and key services. Alerts are in place to ensure that encryption is enabled and any unencrypted data store is identified and remediated in a timely manner.

Upon accepting the terms and conditions and completing the sign-up flow, a new database record and unique identifier are created for a customer account. The unique ID is used thereafter for associating data with the specific customer account. Configurations are in place to ensure that the ID is automatically assigned and unique. The data is logically separated from other customer data using the unique IDs. No database details are used for multiple cloud IDs to ensure this segregation between customers.

A Zero Trust infrastructure is implemented to place endpoints into a tiered network (High, Low, Open) based on their security posture and the type of device. Applications added to the Single Sign-On (SSO) platform are tiered according to the Zero Trust policy. Endpoints cannot access applications via the SSO platform unless they are placed on the same or higher tier as the application. High-tier applications have security requirements that include, but are not limited to, effective malware protection, local drive encryption, and up to date operating system versions.

Firewall rules have been implemented and policy rules have been configured to restrict access to unnecessary ports, protocols, and services. Atlassian has implemented company-wide firewall rules that are managed centrally by the Global Edge team. Individual products and services manage key Internet

Protocol (IP) ports security policy roles to ensure that only authorized ports are in use. Any changes to firewall rules at the Global Edge, product, or service level must go through a peer review and approval process.

### Database

Atlassian products utilize logically separate databases for each product instance. The data is segregated by tenant at the application layer using a unique identifier to query customer data.

The databases implemented by Atlassian include independent synchronous replicas in multiple Availability Zones (AZs) within the same region to mitigate the risk of data loss due to hardware failure. The primary datastore used within the Atlassian environment consists of Amazon Relational Database Service (Amazon RDS) clusters located within the private network hosted in AWS. Excluding Jira Align, the cluster is shared, and its nodes are distributed across multiple AZs to provide fault tolerance and redundancy. Jira Align provides a dedicated cluster through a dedicated VPC.

Backups are retained at a minimum for 30 days to provide redundancy and enable point-in-time data recovery (PITR). The data is stored in both the document storage platform (Media Platform) and Amazon Simple Storage Service (Amazon S3). Amazon S3 is utilized as a file service for user attachments, backups, and log archives and is the operational responsibility of Amazon.

## Software

The following table lists the software, services and tools that support the control environment of the Atlassian Cloud products:

| Function | Name | Component |
|---|---|---|
| Hosting Systems | Amazon EC2 | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |
| | Kubernetes on top of Amazon EC2 | Assets, Bitbucket Pipelines, Jira Service Management |
| | CentOS | Compass |
| | Lambda | Forge |
| Storage and Database | Amazon RDS for PostgreSQL | Assets, Atlas, Atlassian Analytics, Compass, Confluence Cloud, Forge, Jira Cloud, Jira Product Discovery, Jira Service Management, and Jira Work Management |
| | Amazon RDS | Forge, Jira Align, Statuspage, and Trello |
| | Dynamo Database | Assets, Automation for Jira, Bitbucket Pipelines, Compass, Confluence Cloud, Forge, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, and Opsgenie |
| | Amazon S3 | Assets, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |

| Function | Name | Component |
|---|---|---|
| | Amazon S3 Glacier | Trello |
| | Aurora | Automation for Jira, Bitbucket Cloud, and Opsgenie |
| | AWS Key Management Service (AWS KMS) | Opsgenie |
| | Azure Database | Jira Align |
| | MongoDB | Halp and Trello |
| | NetApp cloud volume service (CVS) | Bitbucket Cloud |
| | Redis | Atlas and Opsgenie |
| Network | Amazon VPC | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |
| | Amazon Load Balancers (ALB) | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, and Statuspage |
| | Cloudflare | Halp, Jira Align |
| | Corporate firewall | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |
| | Amazon CloudFront | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, and Opsgenie |
| | AWS Web Application Firewall (AWS WAF) | Assets, Forge, Insight, Jira Service Management, and Opsgenie |
| | HAProxy | Trello |
| | Kubernetes | Opsgenie |
| Application Cache | Amazon ElastiCache | Assets, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Compass, Confluence Cloud, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, and Statuspage |
| | Redis | Atlas, Bitbucket Pipelines, Forge, and Opsgenie |

| Function | Name | Component |
|---|---|---|
| Search and Analytics | Amazon Elasticsearch Service (Elasticsearch) | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Jira Cloud, Jira Service Management, Jira Product Discovery, Jira Work Management, and Opsgenie |
| | OpenSearch | Trello |
| Messaging | Amazon Simple Queue Service (Amazon SQS) | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, and Opsgenie |
| | Kinesis | Forge and Opsgenie |
| | Amazon Simple Notification Service (Amazon SNS) | Bitbucket Pipelines and Opsgenie |
| | Slack | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |
| | Microsoft Teams | Halp |
| Build, Release, and Continuous Integration Systems | Deployment Bamboo | Assets, Automation for Jira, Confluence Cloud, Halp, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Statuspage, and Trello |
| | Appveyor | Jira Align |
| | Bitbucket Cloud | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |
| | Bitbucket Pipelines | Assets, Atlas, Atlassian Analytics, Bitbucket Cloud, Bitbucket Pipelines, Compass, Data Lake, Forge, Halp, Jira Service Management |
| | Puppet | Trello |
| | Testory | Jira Align |
| | Tokenator | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |
| | Octopus | Jira Align |

| Function | Name | Component |
|---|---|---|
| Access Management | Active Directory (AD) | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |
| | Idaptive SSO | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |
| | Duo two-factor authentication (2FA) | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |
| | 1Password | Halp |
| Monitoring and Alerting | AppDynamics | Jira Align |
| | AWS CloudTrail | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |
| | EventBus | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |
| | New Relic | Bitbucket Cloud and Opsgenie |
| | Nagios | Trello |
| | AlertLogic | Jira Align |
| | Opsgenie | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |
| | Pendo | Jira Align |
| | Pingdom | Statuspage |
| | Pollinator | Jira Align, Statuspage |
| | SignalFX | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |

| Function | Name | Component |
|---|---|---|
| | Splunk | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |
| | Sentry | Jira Align, Halp |
| | Proofpoint | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |
| Customer Support and Communication | Atlassian Community | Data Lake |
| | Intercom | Opsgenie |
| | Statuspage | Assets, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Forge, Jira Align, Jira Cloud, Jira Service Management, Jira Work Management, and Opsgenie |
| Vulnerability Scanning | Cloud Conformity | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |
| | BugCrowd | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |
| | CrowdStrike | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Service Management, Jira Product Discovery, Jira Work Management, Opsgenie, Statuspage, and Trello |
| | Tenable | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |
| | Snyk | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |

| Function | Name | Component |
|---|---|---|
| | Security Assistant | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |
| Human Resources (HR) | Workday | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |
| | Lever | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |
| Learning, Training, and Development | Absorb | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |
| | Learning Central | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |
| | Haekka | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |
| | Degreed | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |
| | Get Abstract | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |
| | LinkedIn Learning | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |

| Function | Name | Component |
|---|---|---|
| | Learndot | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |
| | Intellum | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |
| Notifications | Nexmo | Opsgenie |
| | Mailgun | Opsgenie |
| | Twilio | Opsgenie |
| | Pubnub | Opsgenie |
| | SES | Jira Align |
| Asset Management | Jamf Pro | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |
| | Workspace One | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |
| | Bitlocker | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |
| | Filevault | Assets, Atlas, Atlassian Analytics, Automation for Jira, Bitbucket Cloud, Bitbucket Pipelines, Compass, Confluence Cloud, Data Lake, Forge, Halp, Jira Align, Jira Cloud, Jira Product Discovery, Jira Service Management, Jira Work Management, Opsgenie, Statuspage, and Trello |

AWS and Azure are third-party vendors that provide physical and environmental safeguards, infrastructure support, management, and storage services. Atlassian has identified the complementary subservice organization controls of AWS and Azure to achieve the applicable trust services criteria.

MongoDB is a third-party vendor that provides database management services. Atlassian has identified the complementary subservice organization controls of MongoDB to achieve the applicable trust services criteria.

The other third-party vendors mentioned above are only applicable to support specific controls.

## People

The Company develops, manages, and secures the Atlassian Cloud Products 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 initiatives, establishing and accomplishing goals, and managing objectives |
| People (in partnership with the people leaders) | Responsible for determining career growth and performance strategy, talent acquisition, continuing education paths, total rewards, and workplace experiences |
| Finance | Responsible for financial, accounting, tax, internal audit, investor relations, procurement, and treasury |
| Legal | Responsible for matters related to corporate development, confidentiality, general counsel operations, and public relations |
| Engineering | Responsible for the development, testing, deployment, and maintenance of new code for the Atlassian Cloud Products |
| Trust | Responsible for managing access controls, the security of the production environment, enterprise risk management, business continuity, and compliance for the Atlassian Cloud Products |
| Platform and Enterprise Cloud | Responsible for architecting, building, and maintaining, the Atlassian Cloud Products |
| Ecosystem | Responsible for third party connectivity platforms and applications |
| Foundation | Responsible for harnessing the resources of Atlassian to champion organizations who believe that education is the key to eliminating disadvantage |
| Product | Responsible for overseeing the product life cycle, including adding new product functionality |

The following organizational chart reflects the Company’s internal structure related to the groups discussed above:

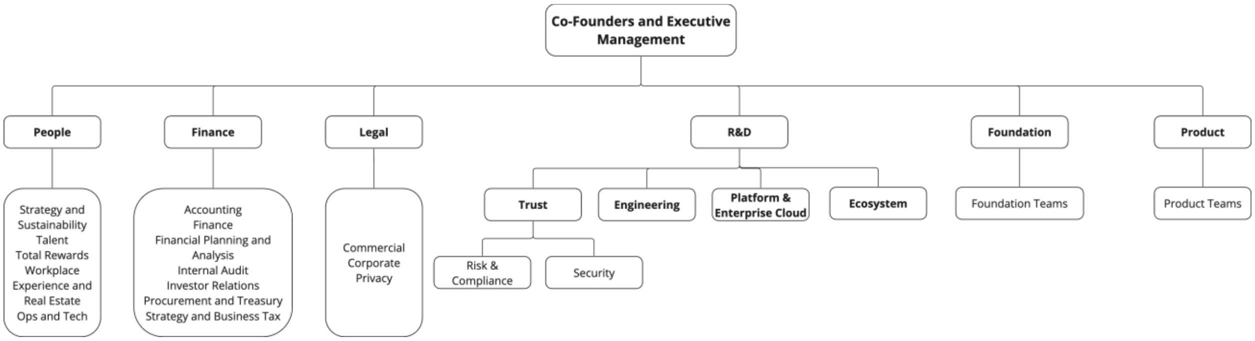

*Figure 1: Atlassian Organizational Chart*

# 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
- Providing 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.

| 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 all personnel. |
| 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, it 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 that 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 Management team. Policy owners can approve exceptions for a period no longer than one (1) year.

### Policy Review Process

In order to advance a policy, standard, guideline, or standard operating procedure to be publicly available internally to all Atlassian employees, each document goes through a review process. The review process follows Atlassian's internal process in which 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 Classification and Confidentiality of Information

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

- Information should be classified in terms of legal requirements, value, and criticality to Atlassian
- Information should be labeled to manage appropriate handling
- All removable media should be managed 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** |
| Restricted | Information that would be very damaging and would cause loss of trust with customers and present legal risk to Atlassian and/or customers if mishandled | Customer data<br>Sensitive company accounting data (e.g., non-public financial data, including consolidated revenue, expenses, cash flow, and earnings guidance prior to release)<br>Decryption keys, passwords, or other access control mechanisms protecting data at this level<br>United States Social Security numbers (customers or employees)<br>Customer and employee Personally Identifiable Information (PII)<br>Employee personal, bank, and salary details |
| Protected | Information that could cause **loss of trust** with customers or present **legal risk** to Atlassian if mishandled | Atlassian Account ID |
| Confidential | Information that would likely be damaging and could cause loss of trust with our customers if mishandled | Confidential personal data elements<br>Information related to business plans or deals<br>Information under a Non-Disclosure Agreement (NDA)<br>Descriptions of unresolved security issues in Atlassian products<br>Third party closed-source code |

| Data Classification | | |
|---|---|---|
| **Rating** | **Description** | **Examples** |
| Internal | Information internal to Atlassian that could be potentially damaging to Atlassian and/or customers if mishandled | Most Confluence pages<br>Most information stored in Jira<br>Unreleased source code for Atlassian products<br>Unapproved drafts of public communications |
| Public | Data that is freely available to the public and presents no risk | Approved public communications<br>Information on www.atlassian.com or other public web properties |

## 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, 2022 to September 30, 2023.

# 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 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. *Information and communication:* 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 and privacy categories.

# Control Environment

## Integrity, Ethical Values and Competence

Integrity, ethical values, and competence are essential components of Atlassian's control environment. All Atlassian employees must acknowledge the Code of Business Conduct and Ethics. The HR Operations team is responsible for reviewing and monitoring compliance with these policies and agreements and ensuring that background screening procedures are carried out promptly.

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

Atlassian's Board of Directors and subcommittees meet annually to review committee charters, corporate governance, and strategic operational objectives. Meeting minutes are recorded with details on participants and dates. Targets are conveyed to product groups for execution by Management, with progress evaluated quarterly. Audit committee information is accessible on Atlassian's Investor website, including roles, responsibilities, key activities, meetings, qualifications for Financial Expert role, meeting calendar, and agenda developed annually with results published after each meeting.

### Board and Governance Committee Charter

The Board of Directors and its subcommittees (Audit, Nominating and Governance) annually review the Board, Audit, and Nominating and Governance Committee Charters that outline their respective roles, responsibilities, meeting frequency, participants, member qualifications, discussion topics, and key activities. The Nominating and Governance Committee charter defines the process of identifying and reviewing candidates for the Board of Directors.

### Management’s Philosophy and Operating Style

At Atlassian, Executive and Senior Management are continuously engaged in a controlled environment. The Risk and Compliance team follows specific standards for security, availability, quality, reliability, and confidentiality. Customized tools assist in identifying risks and findings while workflows ensure proper tracking of activities. An Enterprise Risk Management process modeled after ISO 31000:2009 is used to create universal control activities that meet multiple standards. This approach promotes operational efficiency and a unified language across the organization.

### Rules of Behavior

Atlassian requires all employees and specified contractors to acknowledge the Code of Business Conduct and Ethics, Insider Trading Policy, Foreign Corrupt Practices Act (FCPA) Agreement, and Anti-Corruption Policy upon hire to ensure that they are aware of their responsibilities and expected behavior. The Code of Business Conduct and Ethics policy is reviewed on an annual basis. Atlassian ensures that all relevant personnel have appropriate access agreements in place.

A hotline for whistleblowers has been established and is available to both external individuals and Atlassian employees. It is included in the Code of Business Conduct and Ethics, which all employees are required to acknowledge. Atlassian adheres to the Policy Violation Investigation Process when conducting investigations that may require disciplinary action, up to and including termination of employment, for individuals who fail to comply. Atlassian also requires its employees to complete anti-harassment training.

### Personnel Management and Termination

Background checks are completed for new employees prior to their start date and a weekly review is conducted to confirm that the CIIA (Confidential Information and Inventions Assignment) has been signed as part of the onboarding process. For external candidates, the hiring manager or Talent Acquisition team reviews and formally approves every offer that is made. The Talent Acquisition team approves offers for interns and graduates due to the bulk nature and timing of these hires.

Atlassian has a documented performance review process in place and reviews employee performance on an annual basis. Growth Plans are 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. Atlassian provides opportunities for professional development via training or tuition reimbursement and online learning management systems.

## Information and Communication

### Internal Audit

The Internal Audit team is responsible for carrying out procedures to confirm adherence to and verification with the internal information security management system. The design of controls and mitigation strategies are reviewed on an annual basis. The outcomes of internal audits are documented, and corrective actions are monitored via reports to management.

### Awareness and Training

Atlassian delivers annual security awareness training to all employees upon commencement of employment and annually thereafter. This program ensures staff are made aware of security risks and regulations. Automated notification reminders are sent to employees and escalated to their managers to make sure training is completed by the respective deadlines.

### Program Management

Atlassian maintains a security policy, which is shared and reviewed annually to ensure that security is appropriately designed and integrated into the system. The policies are posted online, assigned a policy owner, and reviewed at least annually by the designated policy owner or their delegate.

Atlassian has a personnel development program for the security and confidentiality workforce, and training is provided to employees to support their ongoing development and growth. An organizational chart is in place and updated to ensure identification of roles and responsibilities. The organizational chart is reviewed by appropriate Atlassian management and updated as needed.

Atlassian implements a process to ensure that strategic operational objectives are set, reviewed, and properly prioritized. The Executive Management team sets strategic operational objectives quarterly.

### System Security Plan

Atlassian provides detailed documentation on system boundaries, product descriptions, and key services on both the Atlassian intranet and customer-facing website. Internal users and customers are informed of significant changes made to key products and services. Atlassian also communicates changes to confidentiality and security commitments on its Trust Center. For any material changes, an additional notice is also provided.

### Incident Response

Atlassian maintains a company-wide incident management policy that is shared and reviewed on an annual basis. Incident management response procedures and plans are integrated into mission critical business processes and systems to minimize downtime, service degradation, and security risk for customers and internal users. System availability is published to provide assistance to users for the handling and reporting of incidents. Atlassian also provides a variety of methods and channels for customers to report incidents, system vulnerabilities, bugs, and issues related to defects, availability, security, and confidentiality.

## Risk Assessment and Mitigation

### Enterprise Risk Management

Atlassian's framework for enterprise risk management is developed, documented, and reviewed annually to manage risks related to Atlassian's strategy and business objectives. Atlassian has a Risk Management policy that is shared, assigned a policy owner, and reviewed at least annually by the designated policy owner or their delegate. Atlassian has a risk assessment process in place in which risks are documented with a risk rating and assigned a risk owner. Atlassian ensures that risks outside of the acceptable level of risk are monitored and risk assessments are reviewed annually.

### Fraud Risk Assessments

A fraud risk assessment is performed annually by the Head of Risk and Compliance or a delegate. The assessment includes a cross functional survey of employees in areas susceptible to fraud combined with an evaluation of external risks. The report results are evaluated and communicated to executive level management and the Audit Committee.

### Supplier Assessment and Review

Atlassian ensures that its vendors meet security, availability, and confidentiality commitments during the procurement process and on an ongoing basis, as applicable. Atlassian follows a defined process for vendor reviews, which includes an Initial Supplier Risk Assessment, Supplier Due Diligence and Risk Treatment, Contract Management, and Supplier Monitoring. To achieve Atlassian's principal service commitments and system requirements, Atlassian reviews SOC reports at least annually for material third-party services and applications to ensure that controls are appropriate and operating effectively.

## Monitoring

### Vulnerability Management

Atlassian performs vulnerability scanning on a continuous basis. Atlassian ensures that any legitimate vulnerabilities are remediated in accordance with the vulnerability management policy.

### Penetration Testing

Atlassian conducts penetration testing at least annually on all publicly accessible Atlassian products. Bug bounty programs are utilized to detect traditional web application vulnerabilities as well as other vulnerabilities that can have a direct impact. These vulnerabilities are tracked and mitigated until they are resolved.

## Control Activities

### Access Control

Atlassian ensures that access to services, products, cloud service providers, internal systems, and tools is managed in compliance with relevant access control policies. Access is provisioned in line with the principle of least privilege only after approval is documented via a Jira ticket or in the internal Self Service Access Management (SSAM) tool and is reviewed at least semi-annually. Access to the Trello Jumpbox is the only component in the environment that is managed outside of the SSAM tool.

Registration and de-registration of user access is restricted to authorized users via Active Directory group membership, which is automatically assigned based on the user’s department and team. AD contains a subset of groups that 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 member’s assigned groups are updated to reflect a team or department change or termination.

Automatic alerts are generated for role changes made in reassignment or transfer of personnel. User access to products and services is modified as necessary to correspond to these changes. Atlassian also ensures that upon termination, user access to products, production systems, tools, and services is revoked within 8 hours and access to the network is also disabled.

### Identification and Authentication

Atlassian products and services are secured with passwords and multi-factor authentication (MFA). This ensures that only authorized individuals can access cloud services and remote access systems.

Atlassian employees are uniquely identified and authenticated using AD, which enforces password settings in accordance with the password standard. Atlassian's SSO portal (Idaptive) allows users to have a single point of authentication to access multiple applications.

In cases where MFA is not available, a distinct username and password must be provided. MFA is mandatory to access the virtual private network (VPN) from any IP address and when launching an application from Idaptive.

Customers are uniquely identified and authenticated as well using password mechanisms that are controlled by their Atlassian account. Unless an external identity provider is implemented by the customer, customers must meet the minimum password requirements that are controlled via their Atlassian account.

# System Operations

## Boundary Protection

Atlassian has firewall rules in place to restrict access to the production environment. The firewalls are configured to limit unnecessary ports, protocols, and services. Atlassian manages and monitors external interfaces and key internal interfaces to the products and services to prevent unauthorized use or access.

## Malicious Code Protection

Atlassian implements and enforces malware protection on corporate endpoints. An enterprise anti-malware platform provides endpoint protection, centralized reporting, and notifications. Atlassian quarantines any malicious software upon detection of suspicious activities, and incident tickets are created for review and resolved in a timely manner.

## Mobile Devices

Usage restrictions, configuration/connection requirements, and authorization is documented and established for mobile devices.

## Encryption

Atlassian implements cryptographic mechanisms to prevent unauthorized disclosure and modification of data in transit and at rest.

# Change Management

Atlassian ensures that configuration-controlled changes to products, services, and the infrastructure are reviewed, approved, and documented. Change management responsibilities are segregated among designated personnel. Emergency changes undergo a similar process. In the event of a catastrophic failure, Atlassian has break glass procedures in place to bypass MFA required for the VPN and the Atlassian SSO portal (Idaptive).

Configuration changes are documented and monitored for non-compliance. An alert is automatically generated if a change to the peer review enforcement for pull requests occurs.

## Prevention of Unauthorized Changes

Atlassian enforces restrictions on infrastructure access to prevent unauthorized modifications. Only artifacts with a valid signature from build software can be released to the production environment. If unauthorized hardware, software, or firmware components are detected, they are isolated, and access is disabled until the relevant support personnel are notified. IT Asset management software is utilized to enforce hard drive encryption, user authentication requirements, and security patching on MacOS and Windows endpoints.

## Availability

### Contingency Planning and Backups

Atlassian has a disaster recovery policy that has been assigned a policy owner and is reviewed at least annually by the designated policy owner or their delegate. It outlines the purpose, objectives, scope, critical dependencies, recovery time objective/recovery point objective (RTO/RPO), and roles and responsibilities. These details are also available online on the Atlassian Trust Center.

Quarterly disaster recovery tests are conducted and exercises are performed to help disaster response teams walk through various scenarios. Post testing, outputs are captured and analyzed to determine next steps for continued improvement.

Atlassian performs backups at least daily and annual restoration testing of system data for its products and services to ensure that data security, integrity, and reliability are maintained. Capacity management is performed on an ongoing basis by all products. Changes to the availability and processing capacity of the customer-facing service products and key services are internally monitored and adjusted accordingly.

## Confidentiality

### Information Handling and Retention

Atlassian ensures that customer data is deleted within a reasonable time frame upon request or termination of contract. Upon termination of contract, the customer’s account is deactivated after the end of the customer’s current subscription period. Atlassian retains data for deactivated products for up to 60 days after the end of the customer’s current subscription period. Upon deletion, an archive of the data is kept at a minimum for an additional 30 days.

### Access to Customer Data

Customer data is logically isolated through the use of unique identifiers. Access to customer data is granted implicitly through customer support tickets or active incidents. This access is for troubleshooting purposes and is granted via tokens only for a limited period of time or until the incident is closed. Customer support tickets can only be submitted by individuals delegated as administrators within Atlassian Admin.

# Complementary User Entity Controls (CUECs)

The Company’s controls related to the Atlassian Cloud Products cover only a portion of overall internal control for each user entity of the Atlassian Cloud Products. 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, considering the related CUECs identified for the specific criterion. 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.<br>• 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.<br>• Opsgenie-specific - Customers are responsible for setting push notifications to active/on. |
| CC6.1 | • Customers are responsible for configuring their own instance, including the appropriate set-up of their logical security and privacy settings (such as IP allowed listing, 2FA, SSO setup, password settings, and restricting public access).<br>• Customers are responsible for changing their passwords to reflect a minimum length of at least eight (8) characters where they have migrated from another identity service.<br>• Customers are responsible for the safeguarding of their own account access credentials, including passwords or Application Programming Interface (API) keys and tokens. |
| CC6.6<br>CC6.8<br>C1.1<br>C1.2 | • Customers are responsible for security, including virus scans and confidentiality of the data (e.g., media attachments), prior to import or attachment and its ongoing monitoring after data has been uploaded. |
| CC6.2<br>CC6.3 | • Customers are responsible for managing access rights, including privileged access.<br>• Customers are responsible for requesting, approving, and monitoring Atlassian's customer support access to their account. |
| CC6.2<br>CC6.3<br>C1.2 | • Customers are responsible for requesting removal of their account. |
| CC6.6<br>CC6.7<br>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. |
| A1.2 | • Bitbucket-specific - Customers are responsible for performing periodic backups of their accounts and repositories for data beyond seven (7) days.<br>• Forge-specific - Application developers are responsible for maintaining backups of their application code. |

# Subservice Organizations and Complementary Subservice Organization Controls (CSOCs)

The Company uses AWS and Azure as subservice organizations for data center colocation services. The Company also uses MongoDB as a subservice organization for database hosting services. The Company's controls related to the Atlassian Cloud Products cover only a portion of the overall internal control for each user entity of the Atlassian Cloud Products. The description does not extend to the colocation services for

IT infrastructure provided by the subservice organization. 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, Azure, and MongoDB.

The following table outlines the individual colocation hosting and database hosting services responsibilities of the subservice organizations:

| Subservice Organization | Products Applicable to the Subservice Organization |
|---|---|
| AWS (data hosting) | Jira Cloud, Confluence Cloud, Bitbucket Cloud, Bitbucket Pipelines, Opsgenie, Forge, Atlas, Jira Align, Jira Service Management, Jira Product Discovery, Jira Work Management, Data Lake, Atlassian Analytics, Compass, Statuspage, Trello, Assets, Automation for Jira, Halp |
| Azure (data hosting – if elected by customer) | Jira Align |
| MongoDB (database hosting) | Halp, Trello |

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 Azure related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. AWS' and Azure's physical security controls should mitigate the risk of unauthorized access to the hosting facilities. AWS' and Azure's environmental protection controls should mitigate the risk of fires, power loss, climate, and temperature variabilities. CSOCs are expected to be in place at MongoDB related to database logical isolation and security related to segmentation. MongoDB's controls should mitigate the risk of unauthorized access to the in-scope databases.

Company management receives and reviews the AWS, Azure, and MongoDB SOC 2 reports annually. In addition, through its operational activities, Company management monitors the services performed by AWS, Azure, 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 facility, and relay any issues or concerns to AWS, Azure, and MongoDB management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to the Atlassian Cloud Products 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, considering the related CSOCs expected to be implemented at AWS, Azure, and MongoDB as described below.

| Criteria | Complementary Subservice Organization Controls |
|---|---|
| CC6.1<br>CC6.2<br>CC6.3 | • AWS and Azure are responsible for IT access above least privileged, including administrator access and are responsible for approval by appropriate personnel prior to access provisioning.<br>• AWS and Azure are responsible for privileged IT access reviews on a regular basis.<br>• AWS and Azure are responsible for timely revocation of user access upon termination.<br>• AWS and Azure are responsible for encrypting data in transit and at rest.<br>• MongoDB is responsible for encrypting data at rest.<br>• MongoDB is responsible for logically isolating data through the use of unique identifiers. |

| Criteria | Complementary Subservice Organization Controls |
|---|---|
| CC6.4 | • AWS and Azure are responsible for restricting physical access to the computer rooms that house the entity's IT resources, servers, and related hardware to authorized individuals through a badge access system or equivalent that is monitored by video surveillance.<br>• AWS and Azure are responsible for approving requests for physical access privileges from an authorized individual.<br>• AWS and Azure are responsible for requiring visitors to be signed in by an authorized workforce member before gaining entry and always escorting them. |
| CC6.5<br>CC6.7 | • AWS and Azure are responsible for securely decommissioning and physically destroying production assets in their control. |
| CC7.1<br>CC7.2<br>CC7.3 | • AWS and Azure are responsible for implementing and monitoring electronic intrusion detection systems that can detect breaches into data center server locations.<br>• AWS and Azure are responsible for documenting procedures for the identification and escalation of potential security breaches. |
| CC7.2<br>A1.2 | • AWS and Azure are responsible for installing environmental protection that includes the following: cooling systems, battery and generator backups, smoke detection, and dry pipe sprinklers.<br>• AWS and Azure are responsible for monitoring the environmental protection equipment for incidents or events that impact assets. |
| CC8.1 | • AWS and Azure 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 (With Revised Points of Focus—2022)* (2017 TSC) 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 the Atlassian Cloud Products are used to provide the service from October 1, 2022 to September 30, 2023.

# Report Use

The description does not omit or distort information relevant to the Atlassian Cloud Products 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 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 Business Conduct and Ethics, 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, 2022 to September 30, 2023. 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 the Atlassian Cloud Products 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 | 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. | | |
| | A comprehensive Code of Business Conduct and Ethics describes employee and contractor responsibilities and expected behavior regarding data and information system usage. The policy is shared and reviewed on an annual basis. | Inspected the Code of Business Conduct and Ethics policy available internally via the Company intranet to determine that the policy was in place to describe employee and contractor responsibilities and expected behavior regarding data and information system usage, was shared with employees, and was reviewed during the period. | No exceptions noted. |
| | Employees acknowledge the Code of Business Conduct and Ethics policy upon hire. | Inspected acknowledgements for a sample of new employees to determine that new employees acknowledged that they had read and agreed to the Code of Business Conduct and Ethics policy upon hire. | Exceptions noted. 1 out of a sample of 44 new employees did not acknowledge the Code of Business Conduct and Ethics policy upon hire. |
| | Employee performance is reviewed on an annual basis. | Inspected performance appraisal documentation for a sample of employees to determine that performance appraisals were completed during the period. | No exceptions noted. |
| | The Company has documented disciplinary actions in a formalized sanctions policy for employees and contractors who violate the Code of Business Conduct and Ethics. | Inspected the Code of Business Conduct and Ethics to determine that the Company had documented disciplinary actions in a formalized sanctions policy for employees and contractors who violated the Code of Business Conduct and Ethics. | No exceptions noted. |

## Control Environment

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor’s Tests | Results of Tests |
|---|---|---|---|
| | Background checks are performed prior to an employee’s start date in compliance with local laws and regulations. | Inspected background check completion evidence for a sample of new employees to determine that background checks were performed prior to their start date in compliance with local laws and regulations. | No exceptions noted. |
| | Employees are required to sign Confidential Information and Inventions Assignments (CIIAs) as part of the onboarding process. | Inspected signed CIIAs for a sample of new employees to determine that agreements were signed as part of the onboarding process. | No exceptions noted. |
| | A weekly review is performed to determine that the CIIA and background checks are completed for new employees as part of onboarding procedures. | Inspected weekly reviews for a sample of weeks to determine that a weekly review of CIIA acknowledgement and background checks was completed. | No exceptions noted. |
| **CC1.2** | The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control. | | |
| | The Board and Committee Charter outlines the roles, responsibilities, and key activities of the board. | Inspected the Board and Committee Charter and meetings to determine that the roles, responsibilities, and key activities of the board were defined. | No exceptions noted. |
| | The Audit Committee Charter outlines the roles, responsibilities, and key activities of the Audit Committee. | Inspected the Audit Committee Charter to determine that the roles, responsibilities, and key activities of the Audit Committee were defined. | No exceptions noted. |
| | Atlassian's Board of Directors and subcommittees meet annually to review committee charters, corporate governance, and strategic operational objectives. Meeting minutes are recorded with details on participants and dates. | Inspected meeting minutes to determine that the Atlassian Board of Directors and subcommittees met during the period to review committee charters, corporate governance, and strategic operational objectives, and included details on participants and dates. | No exceptions noted. |

**Control Environment**

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| | The Nominating and Governance Committee Charter outlines the roles, responsibilities, and key activities of the Nominating and Governance Committee. | Inspected the Nominating and Governance Committee Charter to determine that it outlined the roles, responsibilities, and key activities of the Nominating and Governance Committee. | No exceptions noted. |
| **CC1.3** | Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. | | |
| | An organizational chart is in place and updated to ensure identification of roles and responsibilities. | Inspected the organizational chart and review documentation to determine that an organizational chart was in place and updated during the period to ensure identification of roles and responsibilities. | No exceptions noted. |
| | Management has established defined roles and responsibilities to oversee the implementation of the security and control environment. | Inspected the Atlassian 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. |
| | The hiring manager reviews and approves employee job descriptions. | Inspected job description posting approvals for a sample of postings to determine job descriptions were 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 | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| **CC1.4** | The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. | | |
| | Employees are required to complete security awareness training at least annually. | Inspected training completion evidence for a sample of employees to determine that employees were required to complete security awareness training during the period. | No exceptions noted. |
| | A personnel development program for security and confidentiality has been established. | Inspected training tools made available to all employees to determine that a personnel development program for security and confidentiality had been established. | No exceptions noted. |
| | The hiring manager reviews and approves employee job descriptions. | Inspected job description posting approvals for a sample of postings to determine job descriptions were 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. |
| | Employee performance is reviewed on an annual basis. | Inspected performance appraisal documentation for a sample of employees to determine that performance appraisals were completed during the period. | No exceptions noted. |
| | External candidates are formally approved prior to receiving an offer. | Inspected approval documentation for a sample of new hires to determine that external candidates were formally approved prior to receiving an offer. | No exceptions noted. |

| Control Environment | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| **CC1.5** | The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives. | | |
| | Employee performance is reviewed on an annual basis. | Inspected performance appraisal documentation for a sample of employees to determine that performance appraisals were completed during the period. | No exceptions noted. |
| | A comprehensive Code of Business Conduct and Ethics describes employee and contractor responsibilities and expected behavior regarding data and information system usage. The policy is shared and reviewed on an annual basis. | Inspected the Code of Business Conduct and Ethics policy available internally via the Company intranet to determine that the policy was in place to describe employee and contractor responsibilities and expected behavior regarding data and information system usage, was shared with employees, and was reviewed during the period. | No exceptions noted. |
| | Employees acknowledge the Code of Business Conduct and Ethics policy upon hire. | Inspected acknowledgements for a sample of new employees to determine that new employees acknowledged that they had read and agreed to the Code of Business Conduct and Ethics policy upon hire. | Exceptions noted. 1 out of a sample of 44 new employees did not acknowledge the Code of Business Conduct and Ethics policy upon hire. |
| | The Company has documented disciplinary actions in a formalized sanctions policy for employees and contractors who violate the Code of Business Conduct and Ethics. | Inspected the Code of Business Conduct and Ethics to determine that the Company had documented disciplinary actions in a formalized sanctions policy for employees and contractors who violated the Code of Business Conduct and Ethics. | No exceptions noted. |

**Control Environment**

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor’s Tests | Results of Tests |
|---|---|---|---|
| | The hiring manager reviews and approves employee job descriptions. | Inspected job description posting approvals for a sample of postings to determine job descriptions were 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. |

## Information and Communication

| TSC Reference | 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. | | |
| | Internal audits are performed annually, results are communicated to management and the Audit Committee, and corrective actions are monitored. | Inspected the Atlassian Security Policy to determine internal audits were required to be performed annually, and results must be communicated to management and the Audit Committee. | No exceptions noted. |
| | | Inspected internal audit results to determine an internal audit was performed during the period and corrective actions were monitored and communicated to management and the Audit Committee. | No exceptions noted. |
| | Vulnerability scanning is performed on a continuous basis. | Inspected vulnerability scanning configurations to determine vulnerability scanning is performed on a continuous basis. | No exceptions noted. |
| | Vulnerabilities identified in the vulnerability scans and penetration testing are remediated in accordance with the threat and vulnerability management policy. | Inspected remediation plans for a sample of vulnerabilities identified in the vulnerability scans and annual penetration test to determine that remediation plans were developed and changes were implemented to remediate all vulnerabilities identified during the continuous scans and penetration test in accordance with the threat and vulnerability management policy. | No exceptions noted. |
| | 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. |

## Information and Communication

| TSC Reference | 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. | | |
| | Employees are required to complete security awareness training at least annually. | Inspected training completion evidence for a sample of employees to determine that employees were required to complete security awareness training during the period. | No exceptions noted. |
| | Management has established defined roles and responsibilities to oversee the implementation of the security and control environment. | Inspected the Atlassian 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. |
| | The hiring manager reviews and approves employee job descriptions. | Inspected job description posting approvals for a sample of postings to determine job descriptions were 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. |
| | A whistleblower process is established and accessible to both external individuals and employees. | Inspected the whistleblower hotline documentation to determine that a whistleblower process was established and accessible to both external individuals and employees. | No exceptions noted. |
| | The Executive Team reviews, sets, and/or revises strategic operational objectives quarterly. The targets are cascaded down into each of the product groups for execution by the Management Team. | Inspected strategy and planning documentation for a sample of quarters to determine that the Executive team set strategic operational objectives quarterly that were cascaded down into each of the product groups for execution by the Management Team. | No exceptions noted. |

### Information and Communication

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| | System boundaries, product descriptions, and key services are documented in detail on both the Atlassian intranet and the customer-facing website. | Inspected Atlassian intranet and customer-facing websites to determine that system boundaries, product descriptions, and key services were documented in detail on both the Atlassian intranet and the customer-facing website. | No exceptions noted. |
| | Significant changes made to key products and services are communicated to internal users and customers. | Inspected internal and external Atlassian sites to determine that significant changes made to key products and services were communicated to internal users and customers. | No exceptions noted. |
| **CC2.3** | The entity communicates with external parties regarding matters affecting the functioning of internal control. | | |
| | The cloud terms of service (ToS) and product-specific ToS communicate Atlassian's commitments and the customer responsibilities. The ToS are published on the Atlassian customer-facing website and any changes are communicated. | Inspected the Atlassian cloud ToS and product-specific ToS to determine that the Company's commitments and the customer responsibilities were communicated to customers via the customer-facing website. | No exceptions noted. |
| | Vendor agreements, including any security, availability, and confidentiality commitments, are reviewed during the procurement process for all critical vendors. | Inspected contracts for a sample of critical vendors to determine that vendor agreements, including any security, availability, and confidentiality commitments, were reviewed during the procurement process. | No exceptions noted. |
| | Significant changes made to key products and services are communicated to internal users and customers. | Inspected internal and external Atlassian sites to determine that significant changes made to key products and services were communicated to internal users and customers. | No exceptions noted. |

| Information and Communication | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | Users may report bugs, defects, or availability, security, and confidentiality issues. | Inspected the customer reporting portal to determine that users were able to report bugs, defects, and availability, security and confidentiality issues. | No exceptions noted. |
| | System availability is published to provide assistance to users for the handling and reporting of incidents. | Inspected the Atlassian status page to determine that system availability was published to provide assistance to users for the handling and reporting of incidents | No exceptions noted. |
| | Atlassian communicates changes to confidentiality and security commitments. | Inspected the Atlassian website to determine changes to confidentiality and security commitments were communicated. | No exceptions noted. |

## Risk Assessment

| TSC Reference | 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. | | |
| | The design of controls and mitigation strategies are reviewed annually, including identifying risks and recommending changes in the control environment. | Inspected the Atlassian Risk and Compliance review documentation to determine that the design of controls and mitigation strategies were reviewed during the period and included identifying risks and recommended changes in the control environment. | No exceptions noted. |
| | A Risk Management policy is made available to employees and reviewed annually. | Inspected the Risk Management policy to determine if the policy was made available to employees and reviewed during the period. | No exceptions noted. |
| | Atlassian has defined an Enterprise Risk Management (ERM) process and conducts an enterprise risk assessment annually, which includes key product stakeholders. | Inspected the ERM Program to determine that an ERM process was defined. | No exceptions noted. |
| | | Inspected the ERM risk assessment documentation to determine that an enterprise risk assessment was performed during the period that included key product stakeholders. | No exceptions noted. |
| **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. | | |
| | A Risk Management policy is made available to employees and reviewed annually. | Inspected the Risk Management policy to determine if the policy was made available to employees and reviewed during the period. | No exceptions noted. |
| | Atlassian has defined an Enterprise Risk Management (ERM) process and conducts an enterprise risk assessment annually, which includes key product stakeholders. | Inspected the ERM Program to determine that an ERM process was defined. | No exceptions noted. |
| | | Inspected the ERM risk assessment documentation to determine that an enterprise risk assessment was performed during the period that included key product stakeholders. | No exceptions noted. |

## Risk Assessment

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor’s Tests | Results of Tests |
|---|---|---|---|
| | A fraud risk assessment is performed annually by the Director of Risk and Compliance or delegate. A cross-functional survey of employees in areas susceptible to fraud is conducted and combined with an evaluation of external risks. The report results are evaluated and included within the enterprise risk assessment which is communicated to the board and executive level managers annually. | Inspected the fraud risk assessment to determine that a fraud risk assessment was performed during the period by the Director of Risk and Compliance or delegate during the period and results were included as a part of the enterprise risk assessment, which was communicated to the board and executive level managers. | 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 and included within the enterprise risk assessment. | No exceptions noted. |
| | A disaster recovery policy is shared on the Company intranet and reviewed on an annual basis. | Inspected the disaster recovery policy and Company intranet to determine the disaster recovery policy was reviewed during the period and shared on the Company intranet. | No exceptions noted. |
| | A disaster recovery plan is in place and tested quarterly. | Inspected the disaster recovery plan and tests for a sample of quarters to determine that a disaster recovery plan was in place for all in-scope systems and tested on a quarterly basis. | No exceptions noted. |
| **CC3.3** | The entity considers the potential for fraud in assessing risks to the achievement of objectives. | | |
| | A Risk Management policy is made available to employees and reviewed annually. | Inspected the Risk Management policy to determine if the policy was made available to employees and reviewed during the period. | No exceptions noted. |

**Risk Assessment**

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| | Atlassian has defined an Enterprise Risk Management (ERM) process and conducts an enterprise risk assessment annually, which includes key product stakeholders. | Inspected the ERM Program to determine that an ERM process was defined. | No exceptions noted. |
| | | Inspected the ERM risk assessment documentation to determine that an enterprise risk assessment was performed during the period that included key product stakeholders. | No exceptions noted. |
| | A fraud risk assessment is performed annually by the Director of Risk and Compliance or delegate. A cross-functional survey of employees in areas susceptible to fraud is conducted and combined with an evaluation of external risks. The report results are evaluated and included within the enterprise risk assessment which is communicated to the board and executive level managers annually. | Inspected the fraud risk assessment to determine that a fraud risk assessment was performed during the period by the Director of Risk and Compliance or delegate during the period and results were included as a part of the enterprise risk assessment, which was communicated to the board and executive level managers. | 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 and included within the enterprise risk assessment. | No exceptions noted. |
| **CC3.4** | The entity identifies and assesses changes that could significantly impact the system of internal control. | | |
| | A Risk Management policy is made available to employees and reviewed annually. | Inspected the Risk Management policy to determine if the policy was made available to employees and reviewed during the period. | No exceptions noted. |

## Risk Assessment

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| | Atlassian has defined an Enterprise Risk Management (ERM) process and conducts an enterprise risk assessment annually, which includes key product stakeholders. | Inspected the ERM Program to determine that an ERM process was defined. | No exceptions noted. |
| | | Inspected the ERM risk assessment documentation to determine that an enterprise risk assessment was performed during the period that included key product stakeholders. | No exceptions noted. |
| | A fraud risk assessment is performed annually by the Director of Risk and Compliance or delegate. A cross-functional survey of employees in areas susceptible to fraud is conducted and combined with an evaluation of external risks. The report results are evaluated and included within the enterprise risk assessment which is communicated to the board and executive level managers annually. | Inspected the fraud risk assessment to determine that a fraud risk assessment was performed during the period by the Director of Risk and Compliance or delegate during the period and results were included as a part of the enterprise risk assessment, which was communicated to the board and executive level managers. | 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 and included within the enterprise risk assessment. | No exceptions noted. |
| | Penetration testing is performed at least annually. | Inspected penetration test results to determine testing was performed during the period. | No exceptions noted. |

| Risk Assessment | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | Vulnerabilities identified in the vulnerability scans and penetration testing are remediated in accordance with the threat and vulnerability management policy. | Inspected remediation plans for a sample of vulnerabilities identified in the vulnerability scans and annual penetration test to determine that remediation plans were developed and changes were implemented to remediate all vulnerabilities identified during the continuous scans and penetration test in accordance with the threat and vulnerability management policy. | No exceptions noted. |

## Monitoring Activities

| TSC Reference | 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. | | |
| | Internal audits are performed annually, results are communicated to management and the Audit Committee, and corrective actions are monitored. | Inspected the Atlassian Security Policy to determine internal audits were required to be performed annually, and results must be communicated to management and the Audit Committee. | No exceptions noted. |
| | | Inspected internal audit results to determine an internal audit was performed during the period and corrective actions were monitored and communicated to Management and the Audit Committee. | No exceptions noted. |
| | Penetration testing is performed at least annually. | Inspected penetration test results to determine testing was performed during the period. | No exceptions noted. |
| | Vulnerability scanning is performed on a continuous basis. | Inspected vulnerability scanning configurations to determine vulnerability scanning is performed on a continuous basis. | No exceptions noted. |
| | Vulnerabilities identified in the vulnerability scans and penetration testing are remediated in accordance with the threat and vulnerability management policy. | Inspected remediation plans for a sample of vulnerabilities identified in the vulnerability scans and annual penetration test to determine that remediation plans were developed and changes were implemented to remediate all vulnerabilities identified during the continuous scans and penetration test in accordance with the threat and vulnerability management policy. | No exceptions noted. |

| Monitoring Activities | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | SOC 2 reports of critical vendors are reviewed annually. | Inspected SOC 2 report review documentation for a sample of critical vendors to determine that SOC 2 reports of critical vendors were reviewed during the period. | No exceptions noted. |
| | Suppliers who host or process data undergo an assessment to ensure security and confidentiality requirements are met. | Inspected attestation review documentation for all subservice organizations to determine that suppliers who host or process data underwent an assessment to ensure security and confidentiality requirements were met. | 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. | | |
| | Internal audits are performed annually, results are communicated to management and the Audit Committee, and corrective actions are monitored. | Inspected the Atlassian Security Policy to determine internal audits were required to be performed annually, and results must be communicated to management and the Audit Committee. | No exceptions noted. |
| | | Inspected internal audit results to determine an internal audit was performed during the period and corrective actions were monitored and communicated to Management and the Audit Committee. | No exceptions noted. |
| | SOC 2 reports of critical vendors are reviewed annually. | Inspected SOC 2 report review documentation for a sample of critical vendors to determine that SOC 2 reports of critical vendors were reviewed during the period. | No exceptions noted. |

| Monitoring Activities | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | Suppliers who host or process data undergo an assessment to ensure security and confidentiality requirements are met. | Inspected attestation review documentation for all subservice organizations to determine that suppliers who host or process data underwent an assessment to ensure security and confidentiality requirements were met. | No exceptions noted. |

| Control Activities | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **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. | | |
| | The design of controls and mitigation strategies are reviewed annually, including identifying risks and recommending changes in the control environment. | Inspected the Atlassian Risk and Compliance review documentation to determine that the design of controls and mitigation strategies were reviewed during the period and included identifying risks and recommended changes in the control environment. | No exceptions noted. |
| | Atlassian has defined an Enterprise Risk Management (ERM) process and conducts an enterprise risk assessment annually, which includes key product stakeholders. | Inspected the ERM Program to determine that an ERM process was defined. | No exceptions noted. |
| | | Inspected the ERM risk assessment documentation to determine that an enterprise risk assessment was performed during the period that 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. | | |
| | The design of controls and mitigation strategies are reviewed annually, including identifying risks and recommending changes in the control environment. | Inspected the Atlassian Risk and Compliance review documentation to determine that the design of controls and mitigation strategies were reviewed during the period and included identifying risks and recommended changes in the control environment. | No exceptions noted. |
| | Atlassian has defined an Enterprise Risk Management (ERM) process and conducts an enterprise risk assessment annually, which includes key product stakeholders. | Inspected the ERM Program to determine that an ERM process was defined. | No exceptions noted. |
| | | Inspected the ERM risk assessment documentation to determine that an enterprise risk assessment was performed during the period that included key product stakeholders. | No exceptions noted. |

## Control Activities

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| CC5.3 | The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action. | | |
| | Formal procedures are documented that outline the process the Company's staff follows to perform the following system access control functions:<br>- Adding new users<br>- Modifying an existing user's access<br>- Removing an existing user's access<br>- 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:<br>- Adding new users<br>- Modifying an existing user's access<br>- Removing an existing user's access<br>- Restricting access based on separation of duties and least privilege | No exceptions noted. |
| | A security policy is shared on the Company intranet, and reviewed on an annual basis. | Inspected the Atlassian security policy to determine that the security policy was shared on the Company intranet and reviewed during the period. | No exceptions noted. |
| | All policies are posted and available and reviewed at least annually. | Inspected the company intranet to determine that policies were posted and available online and reviewed during the period. | No exceptions noted. |
| | A Risk Management policy is made available to employees and reviewed annually. | Inspected the Risk Management policy to determine if the policy was made available to employees and reviewed during the period. | No exceptions noted. |
| | 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 backup and recover customer data. | No exceptions noted. |

| Control Activities | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | A data classification policy is in place to support the safety and security of data Atlassian holds. | Inspected the data classification policy to determine that a data classification policy was documented to support the safety and security of data Atlassian holds. | No exceptions noted. |
| | 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. |
| | A vendor management program is in place. Components of this program include:<br>- Maintaining a list of critical vendors<br>- Requirements for critical vendors to maintain their own security practices and procedures<br>- 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:<br>- Maintaining a list of critical vendors<br>- Requirements for critical vendors to maintain their own security practices and procedures<br>- Annually reviewing attestation reports for critical vendors or performing a vendor risk assessment | No exceptions noted. |
| | 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 a formal SDLC methodology was in place that governed the development, acquisition, implementation, changes, and maintenance of information systems and related technology requirements. | No exceptions noted. |
| | Formal data retention and disposal procedures are documented to guide the secure retention and disposal of Company and customer data. | Inspected data retention and disposal procedures to determine that standards for secure retention and disposal of Company and customer data were formally documented. | No exceptions noted. |

| Control Activities | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | An incident management policy is shared on the Company intranet and reviewed on an annual basis. | Inspected the incident management policy and Company intranet to determine that an incident management policy was reviewed during the period and shared on the Company intranet. | No exceptions noted. |

## Logical and Physical Access Controls

| TSC Reference | 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. | | |
| | Customers are uniquely identified and authenticated via unique identifiers. | Reperformed login attempts to determine that customers are uniquely identified and authenticated via unique identifiers. | No exceptions noted. |
| | 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. |
| | 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. |
| | Passwords for in-scope system components are configured according to the Company's policy, which requires the following (unless there is a system limitation):<br>- 8 character minimum<br>- Lockout after 5 invalid attempts | Inspected password configurations and the password policy to determine that passwords for in-scope system components were configured according to the Company's policy (unless there was a system limitation):<br>- 8 character minimum<br>- Lockout after 5 invalid attempts | No exceptions noted. |
| | AD 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. Password settings for Idaptive are enforced by AD via the AD connector for Idaptive. | Inspected AD password configurations and the Atlassian Password Standard to determine that AD enforced password settings in line with the Atlassian Password Standard. | No exceptions noted. |

**Logical and Physical Access Controls**

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| | | 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 password settings for Idaptive were enforced by AD via the AD connector for Idaptive. | No exceptions noted. |
| | 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 are logged. | No exceptions noted. |
| | Customer data is logically isolated through the use of unique identifiers. | Inspected system configurations to determine that customer data was logically isolated through the use of unique identifiers. | No exceptions noted. |
| | A Zero Trust infrastructure is implemented to place endpoints into a tiered network (High, Low, Open) based on their security posture and type of device. Applications added to the SSO platform are tiered according to the Zero Trust policy. Endpoints cannot access applications via the SSO platform unless they are placed on the same/higher tier as the application. | Inspected Zero Trust service tier standards and endpoint minimum baseline configurations to determine applications and endpoints are configured based on tier in compliance with the Zero Trust infrastructure. | No exceptions noted. |
| | | Inspected the Zero Trust service tier standard and the endpoint minimum baseline configuration standard and observed applications on the SSO platform to determine that a Zero Trust infrastructure was implemented to place endpoints into a tiered network (e.g., High, Trusted, Open) based on their security posture and type of device. | No exceptions noted. |

## Logical and Physical Access Controls

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| | | Observed application tiers and endpoint access attempts to determine that applications added to the SSO platform were tiered according to the Zero Trust policy and 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. |
| | Cryptographic mechanisms are implemented or enabled to prevent unauthorized disclosure and modification of data at rest. | Inspected encryption configurations for in scope systems to determine that cryptographic mechanisms were implemented or enabled to prevent unauthorized disclosure and modification of data at rest. | No exceptions noted. |
| **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. | | |
| | Access to customer data requires a valid customer support request or the existence of an active incident that requires access to be resolved. | Inspected system configurations and observed the customer support process to determine that access to customer data required a valid customer support request or the existence of an active incident that required access to be resolved. | No exceptions noted. |
| | AD accounts and permissions are automatically assigned based on user description associated with Workday. | Inspected system configurations to determine that AD accounts and permissions were automatically based on user description associated with Workday. | No exceptions noted. |
| | The provisioning of service and product accounts is based on job role and function and requires manager approval prior to access being provisioned. | Inspected Idaptive account logs to determine that the provisioning of service and product accounts was based on job role and function and required manager approval prior to access being provisioned. | No exceptions noted. |

## Logical and Physical Access Controls

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| | AD 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 AD accounts and network access were automatically disabled within 8 hours from the time an employee was marked as terminated in the HR system. | No exceptions noted. |
| | 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. |
| | Access to internal systems and tools is reviewed at least semi-annually and issues identified are remediated in a timely manner. | Inspected access review documentation for a sample of semi-annual reviews to determine that access reviews of internal systems and tools were performed semi-annually. | No exceptions noted. |
| | | Inspected tickets for a sample of semi-annual access reviews to determine that issues identified in the sampled reviews were remediated in a timely manner. | No exceptions noted. |
| | Access to products and services is reviewed at least semi-annually and issues identified are remediated in a timely manner. | Inspected user access reviews for a sample of semi-annual reviews to determine that access reviews of products and services were performed semi-annually. | No exceptions noted. |
| | | Inspected tickets for a sample of semi-annual access reviews to determine that issues identified in the sampled reviews were remediated in a timely manner. | No exceptions noted. |

## Logical and Physical Access Controls

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor’s Tests | Results of Tests |
|---|---|---|---|
| | Access to the Atlassian internal network and internal tools is restricted to authorized users via the following logical access measures:<br>- Each user account must have an active AD account<br>- Each user account must be a member of the appropriate AD group | Inspected system configurations to determine that access to the Atlassian internal network and internal tools was restricted to authorized users via the following logical access measures:<br>- Each user account must have an active AD account<br>- Each user account must be a member of the appropriate AD group | No exceptions noted. |
| | An automatic alert is sent for any role change between the following groups: Engineering, Customer Support & Success (CSS), or Finance. Appropriateness of access is reviewed and approved. | Inspected system configurations and example alerts to determine that automatic alerts were triggered to the Risk and Compliance Manager and HR for any role change between the following groups: Engineering, CSS, or Finance group. | No exceptions noted. |
| | | Inspected system configurations to determine that the role change would not occur until the appropriateness of the access was reviewed and approved. | No exceptions noted. |
| **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. | | |
| | Access to customer data requires a valid customer support request or the existence of an active incident that requires access to be resolved. | Inspected system configurations and observed the customer support process to determine that access to customer data required a valid customer support request or the existence of an active incident that required access to be resolved. | No exceptions noted. |

## Logical and Physical Access Controls

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| | Privileged access for products and services, including access to migrate to production, is restricted based on job description. | Inspected privileged access listings, inquired of management, and compared each user's level of access to their job role to determine that privileged access for products and services, including access to migrate to production, was restricted based on job description. | No exceptions noted. |
| | Privileged access to internal systems and tools, including access to migrate to production, is restricted based on job description. | Inspected access listings, inquired of management, and compared each user's level of access to their job role to determine that privileged access to internal systems and tools, including access to migrate to production, was restricted based on job description. | No exceptions noted. |
| | Access to the Atlassian internal network and internal tools is restricted to authorized users via the following logical access measures:<br>- Each user account must have an active AD account<br>- Each user account must be a member of the appropriate AD group | Inspected system configurations to determine that access to the Atlassian internal network and internal tools was restricted to authorized users via the following logical access measures:<br>- Each user account must have an active AD account<br>- Each user account must be a member of the appropriate AD group | No exceptions noted. |
| | Only service owners can assign delegates to key infrastructure and services. | Inspected system configurations to determine that only service owners had the ability to grant and remove delegate access to key infrastructure and services. | No exceptions noted. |
| | An automatic alert is sent for any role change between the following groups: Engineering, Customer Support & Success (CSS), or Finance. Appropriateness of access is reviewed and approved. | Inspected system configurations and example alerts to determine that automatic alerts were triggered to the Risk and Compliance Manager and HR for any role change between the following groups: Engineering, CSS, or Finance group. | No exceptions noted. |

| Logical and Physical Access Controls | | | |
|---|---|---|---|
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | | Inspected system configurations to determine that the role change would not occur until the appropriateness of the access was reviewed and approved. | No exceptions noted. |
| | AD accounts and permissions are automatically assigned based on user description associated with Workday. | Inspected system configurations to determine that AD accounts and permissions were automatically based on user description associated with Workday. | No exceptions noted. |
| | The provisioning of service and product accounts is based on job role and function and requires manager approval prior to access being provisioned. | Inspected Idaptive account logs to determine that the provisioning of service and product accounts was based on job role and function and required manager approval prior to access being provisioned. | No exceptions noted. |
| | AD 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 AD accounts and network access were automatically disabled within 8 hours from the time an employee was marked as terminated in the HR system. | No exceptions noted. |
| | Access to internal systems and tools is reviewed at least semi-annually and issues identified are remediated in a timely manner. | Inspected access review documentation for a sample of semi-annual reviews to determine that access reviews of internal systems and tools were performed semi-annually. | No exceptions noted. |
| | | Inspected tickets for a sample of semi-annual access reviews to determine that issues identified in the sampled reviews were remediated in a timely manner. | No exceptions noted. |

| Logical and Physical Access Controls | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | Access to products and services is reviewed at least semi-annually and issues identified are remediated in a timely manner. | Inspected user access reviews for a sample of semi-annual reviews to determine that access reviews of products and services were performed semi-annually. | No exceptions noted. |
| | | Inspected tickets for a sample of semi-annual access reviews to determine that issues identified in the sampled reviews were remediated in a timely manner. | No exceptions noted. |
| | Multi-factor authentication is used for privileged accounts unless there is a system limitation. | Inspected system configurations and observed login attempts to determine that multi-factor authentication was used for privileged accounts unless there is a system limitation. | No exceptions noted. |
| | | Inspected system and password configurations and observed login attempts to determine that the privileged accounts that did not require multi-factor authentication due to a system limitation required a unique username and password in accordance with the password standard. | No exceptions noted. |
| **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. | | |
| | 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. |

## Logical and Physical Access Controls

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| **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. | | |
| | 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 are logged. | No exceptions noted. |
| | Storage media containing sensitive data and licensed software is removed and securely overwritten prior to disposal. | Inspected certificates of destruction for a sample of purged or destroyed media to determine that storage media containing sensitive data and licensed software was removed and securely overwritten prior to disposal. | No exceptions noted. |
| **CC6.6** | The entity implements logical access security measures to protect against threats from sources outside its system boundaries. | | |
| | Multi-factor authentication is used for privileged accounts unless there is a system limitation. | Inspected system configurations and observed login attempts to determine that multi-factor authentication was used for privileged accounts unless there is a system limitation. | No exceptions noted. |
| | | Inspected system and password configurations and observed login attempts to determine that the privileged accounts that did not require multi-factor authentication due to a system limitation required a unique username and password in accordance with the password standard. | No exceptions noted. |
| | External interfaces to the products and services and key internal interfaces are managed and monitored to prevent unauthorized use or access. | Inspected firewall and/or security group rules to determine that external interfaces to the products and services and key internal interfaces were managed and monitored to prevent unauthorized use or access. | No exceptions noted. |

| Logical and Physical Access Controls | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | External interfaces to the infrastructure and shared services and key internal interfaces are managed and monitored to prevent unauthorized use or access. | Inspected firewall and/or security group rules to determine that external interfaces to the infrastructure and shared services and key internal interfaces were managed and monitored to prevent unauthorized use or access. | No exceptions noted. |
| | Infrastructure supporting the service is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. | Inspected patching evidence to determine that infrastructure supporting the service was patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service were hardened against security threats. | No exceptions noted. |
| | IT asset management software is used to enforce hard drive encryption, user authentication requirements, and security patching on Mac/Windows endpoints. | Inspected IT asset management software configurations to determine that tooling was configured to enforce hard drive encryption, user authentication requirements, usage restrictions, authorizations, and security patching for Mac/Windows endpoints. | No exceptions noted. |
| | 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. |
| | 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. |

| Logical and Physical Access Controls | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| **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. | | |
| | IT asset management software is used to enforce hard drive encryption, user authentication requirements, and security patching on Mac/Windows endpoints. | Inspected IT asset management software configurations to determine that tooling was configured to enforce hard drive encryption, user authentication requirements, usage restrictions, authorizations, and security patching for Mac/Windows endpoints. | No exceptions noted. |
| | Cryptographic mechanisms are implemented to prevent unauthorized disclosure and modification of data in transit. | Inspected transmission protocol configurations to determine that cryptographic mechanisms were implemented to prevent unauthorized disclosure and modification of data in transit. | 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. | | |
| | Malicious code protection is implemented on endpoints and servers. | Inspected anti-malware configurations to determine that malicious code protection was implemented on endpoints and servers. | No exceptions noted. |
| | External interfaces to the products and services and key internal interfaces are managed and monitored to prevent unauthorized use or access. | Inspected firewall and/or security group rules to determine that external interfaces to the products and services and key internal interfaces were managed and monitored to prevent unauthorized use or access. | No exceptions noted. |
| | External interfaces to the infrastructure and shared services and key internal interfaces are managed and monitored to prevent unauthorized use or access. | Inspected firewall and/or security group rules to determine that external interfaces to the infrastructure and shared services and key internal interfaces were managed and monitored to prevent unauthorized use or access. | No exceptions noted. |

## Logical and Physical Access Controls

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor’s Tests | Results of Tests |
|---|---|---|---|
| | A Zero Trust infrastructure is implemented to place endpoints into a tiered network (High, Low, Open) based on their security posture and type of device. Applications added to the SSO platform are tiered according to the Zero Trust policy. Endpoints cannot access applications via the SSO platform unless they are placed on the same/higher tier as the application. | Inspected Zero Trust service tier standards and endpoint minimum baseline configurations to determine applications and endpoints are configured based on tier in compliance with the Zero Trust infrastructure. | No exceptions noted. |
| | | Inspected the Zero Trust service tier standard and the endpoint minimum baseline configuration standard and observed applications on the SSO platform to determine that a Zero Trust infrastructure was implemented to place endpoints into a tiered network (e.g., High, Trusted, Open) based on their security posture and type of device. | No exceptions noted. |
| | | Observed application tiers and endpoint access attempts to determine that applications added to the SSO platform were tiered according to the Zero Trust policy and 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. |

| System Operations | | | |
|---|---|---|---|
| **TSC Reference** | **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. | | |
| | Vulnerability scanning is performed on a continuous basis. | Inspected vulnerability scanning configurations to determine vulnerability scanning is performed on a continuous basis. | No exceptions noted. |
| | Vulnerabilities identified in the vulnerability scans and penetration testing are remediated in accordance with the threat and vulnerability management policy. | Inspected remediation plans for a sample of vulnerabilities identified in the vulnerability scans and annual penetration test to determine that remediation plans were developed and changes were implemented to remediate all vulnerabilities identified during the continuous scans and penetration test in accordance with the threat and vulnerability management policy. | No exceptions noted. |
| | Atlassian has defined an Enterprise Risk Management (ERM) process and conducts an enterprise risk assessment annually, which includes key product stakeholders. | Inspected the ERM Program to determine that an ERM process was defined. | No exceptions noted. |
| | | Inspected the ERM risk assessment documentation to determine that an enterprise risk assessment was performed during the period that 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. | | |
| | 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. |

**System Operations**

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor’s Tests | Results of Tests |
|---|---|---|---|
| | Vulnerability scanning is performed on a continuous basis. | Inspected vulnerability scanning configurations to determine vulnerability scanning is performed on a continuous basis. | No exceptions noted. |
| | Vulnerabilities identified in the vulnerability scans and penetration testing are remediated in accordance with the threat and vulnerability management policy. | Inspected remediation plans for a sample of vulnerabilities identified in the vulnerability scans and annual penetration test to determine that remediation plans were developed and changes were implemented to remediate all vulnerabilities identified during the continuous scans and penetration test in accordance with the threat and vulnerability management policy. | No exceptions noted. |
| | Penetration testing is performed at least annually. | Inspected penetration test results to determine testing was performed during the period. | No exceptions noted. |
| | The availability and capacity of each service and its underlying infrastructure are monitored continuously through the use of monitoring tools. Alerts are automatically sent to on-call engineers when early warning thresholds are crossed on key operational metrics. | Inspected the availability and capacity monitoring tools and alert configurations to determine that the availability and capacity of each service and its underlying infrastructure were monitored continuously through the use of monitoring tools and alerts were automatically sent to on-call engineers when early warning thresholds were crossed on key operational metrics. | No exceptions noted. |

**System Operations**

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor’s Tests | Results of Tests |
|---|---|---|---|
| **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. | | |
| | Security events are reviewed and handled in accordance with Incident Management procedures and plans to support Atlassian mission and business processes and systems, which includes the evaluation, logging, tracking, and communication of all events. | Inspected a sample of security events to determine security events were addressed in accordance with Incident Management procedures and plans to support Atlassian mission and business processes and systems, which included the evaluation, logging, tracking, and communication of all events. | No exceptions noted. |
| | Penetration testing is performed at least annually. | Inspected penetration test results to determine testing was performed during the period. | No exceptions noted. |
| | Vulnerability scanning is performed on a continuous basis. | Inspected vulnerability scanning configurations to determine vulnerability scanning is performed on a continuous basis. | No exceptions noted. |
| | Vulnerabilities identified in the vulnerability scans and penetration testing are remediated in accordance with the threat and vulnerability management policy. | Inspected remediation plans for a sample of vulnerabilities identified in the vulnerability scans and annual penetration test to determine that remediation plans were developed and changes were implemented to remediate all vulnerabilities identified during the continuous scans and penetration test in accordance with the threat and vulnerability management policy. | No exceptions noted. |
| | An incident management policy is shared on the Company intranet and reviewed on an annual basis. | Inspected the incident management policy and Company intranet to determine that an incident management policy was reviewed during the period and shared on the Company intranet. | No exceptions noted. |

## System Operations

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| **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. | | |
| | Security incidents are reviewed and handled in accordance with Incident Management procedures and plans to support Atlassian mission and business processes and systems which includes the evaluation, logging, tracking, and communication of all incidents.<br>The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No security incidents occurred during the period. | Inquired of management and inspected security event documentation to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether all security incidents were reviewed and handled in accordance with Incident Management procedures and plans to support Atlassian mission and business processes and systems which included the evaluation, logging, tracking, and communication of all incidents. | Not tested. No security incidents were identified during the period. |
| | An incident management policy is shared on the Company intranet and reviewed on an annual basis. | Inspected the incident management policy and Company intranet to determine that an incident management policy was reviewed during the period and shared on the Company intranet. | No exceptions noted. |
| **CC7.5** | The entity identifies, develops, and implements activities to recover from identified security incidents. | | |
| | A disaster recovery policy is shared on the Company intranet and reviewed on an annual basis. | Inspected the disaster recovery policy and Company intranet to determine the disaster recovery policy was reviewed during the period and shared on the Company intranet. | No exceptions noted. |
| | A disaster recovery plan is in place and tested quarterly. | Inspected the disaster recovery plan and tests for a sample of quarters to determine that a disaster recovery plan was in place for all in-scope systems and tested on a quarterly basis. | No exceptions noted. |

## System Operations

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| | Security incidents are reviewed and handled in accordance with Incident Management procedures and plans to support Atlassian mission and business processes and systems which includes the evaluation, logging, tracking, and communication of all incidents.<br>The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No security incidents occurred during the period. | Inquired of management and inspected security event documentation to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether all security incidents were reviewed and handled in accordance with Incident Management procedures and plans to support Atlassian mission and business processes and systems which included the evaluation, logging, tracking, and communication of all incidents. | Not tested. No security incidents were identified during the period. |
| | An incident management policy is shared on the Company intranet and reviewed on an annual basis. | Inspected the incident management policy and Company intranet to determine that an incident management policy was reviewed during the period and shared on the Company intranet. | No exceptions noted. |

## Change Management

| TSC Reference | 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. | | |
| | Configuration-controlled changes to infrastructure are tested, reviewed, approved, and documented. | Inspected system configurations enforcing requirements to configuration-control changes to infrastructure to determine that configuration-controlled changes to infrastructure were tested, reviewed, approved, and documented. | No exceptions noted. |
| | Configuration-controlled changes to products and services are tested, reviewed, and approved. Change management responsibilities are segregated among designated personnel. | Inspected system configurations enforcing requirements to configuration-control changes to products and services to determine that configuration-control changes to products and services were tested, reviewed, and approved, and that change management responsibilities were segregated among designated personnel. | No exceptions noted. |
| | Configuration changes are documented, and monitored for non-compliance. An alert is automatically generated if a change to the peer review enforcement for pull requests occurs. | Inspected validation check and alert configurations to determine that configuration changes were documented and monitored for non-compliance and generated an alert if a change to peer review enforcement occurred. | No exceptions noted. |
| | Infrastructure access restrictions are configured to prevent unauthorized changes. | Inspected system configurations to determine that infrastructure access was restricted to prevent unauthorized changes. | No exceptions noted. |
| | Privileged access to internal systems and tools, including access to migrate to production, is restricted based on job description. | Inspected access listings, inquired of management, and compared each user's level of access to their job role to determine that privileged access to internal systems and tools, including access to migrate to production, was restricted based on job description. | No exceptions noted. |

## Risk Mitigation

| TSC Reference | 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. | | |
| | A Risk Management policy is made available to employees and reviewed annually. | Inspected the Risk Management policy to determine if the policy was made available to employees and reviewed during the period. | No exceptions noted. |
| | A comprehensive disaster recovery policy is shared, and reviewed on an annual basis. | Inspected the disaster recovery policy and company intranet to determine the disaster recovery policy was reviewed during the period and shared. | No exceptions noted. |
| | A disaster recovery plan is in place and tested quarterly. | Inspected the disaster recovery plan and tests for a sample of quarters to determine that a disaster recovery plan was in place for all in-scope systems and tested on a quarterly basis. | No exceptions noted. |
| | An incident management policy is shared on the Company intranet and reviewed on an annual basis. | Inspected the incident management policy and Company intranet to determine that an incident management policy was reviewed during the period and shared on the Company intranet. | No exceptions noted. |
| | A multi-location strategy is employed for production environments to permit the resumption of operations at other availability zones in the event of the loss of a facility. | Inspected database configurations to determine that a multi-location strategy was employed for production environments to permit the resumption of operations at other availability zones in the event of the loss of a facility. | No exceptions noted. |
| | Databases are replicated to secondary availability zones in real time. Alerts are configured to notify administrators if replication fails. | Inspected replication configurations to determine that databases were replicated to secondary availability zones in real time and that alerts were configured to notify administrators if replication fails. | No exceptions noted. |

**Risk Mitigation**

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor’s Tests | Results of Tests |
|---|---|---|---|
| **CC9.2** | The entity assesses and manages risks associated with vendors and business partners. | | |
| | SOC 2 reports of critical vendors are reviewed annually. | Inspected SOC 2 report review documentation for a sample of critical vendors to determine that SOC 2 reports of critical vendors were reviewed during the period. | No exceptions noted. |
| | Suppliers who host or process data undergo an assessment to ensure security and confidentiality requirements are met. | Inspected attestation review documentation for all subservice organizations to determine that suppliers who host or process data underwent an assessment to ensure security and confidentiality requirements were met. | No exceptions noted. |
| | Vendor agreements, including any security, availability, and confidentiality commitments, are reviewed during the procurement process for all critical vendors. | Inspected contracts for a sample of critical vendors to determine that vendor agreements, including any security, availability, and confidentiality commitments, were reviewed during the procurement process. | No exceptions noted. |

## Additional Criteria for Availability

| Availability | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **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. | | |
| | System availability is published to provide assistance to users for the handling and reporting of incidents. | Inspected the Atlassian status page to determine that system availability was published to provide assistance to users for the handling and reporting of incidents | No exceptions noted. |
| | The availability and capacity of each service and its underlying infrastructure are monitored continuously through the use of monitoring tools. Alerts are automatically sent to on-call engineers when early warning thresholds are crossed on key operational metrics. | Inspected the availability and capacity monitoring tools and alert configurations to determine that the availability and capacity of each service and its underlying infrastructure were monitored continuously through the use of monitoring tools and alerts were automatically sent to on-call engineers when early warning thresholds were crossed on key operational metrics. | 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. | | |
| | A comprehensive disaster recovery policy is shared, and reviewed on an annual basis. | Inspected the disaster recovery policy and company intranet to determine the disaster recovery policy was reviewed during the period and shared. | No exceptions noted. |
| | A disaster recovery plan is in place and tested quarterly. | Inspected the disaster recovery plan and tests for a sample of quarters to determine that a disaster recovery plan was in place for all in-scope systems and tested on a quarterly basis. | No exceptions noted. |

## Availability

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor’s Tests | Results of Tests |
|---|---|---|---|
| | System data of products and services is backed up at least daily. Restoration testing occurs annually to ensure data security and integrity is maintained. | Inspected backup configurations to determine that system data of products and services was backed up at least daily. | No exceptions noted. |
| | | Inspected restoration testing documentation to determine that restoration testing was performed during the period to ensure data security and integrity was maintained. | No exceptions noted. |
| | A multi-location strategy is employed for production environments to permit the resumption of operations at other availability zones in the event of the loss of a facility. | Inspected database configurations to determine that a multi-location strategy was employed for production environments to permit the resumption of operations at other availability zones in the event of the loss of a facility. | No exceptions noted. |
| | Databases are replicated to secondary availability zones in real time. Alerts are configured to notify administrators if replication fails. | Inspected replication configurations to determine that databases were replicated to secondary availability zones in real time and that alerts were configured to notify administrators if replication fails. | No exceptions noted. |
| | 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 backup and recover customer data. | No exceptions noted. |
| **A1.3** | The entity tests recovery plan procedures supporting system recovery to meet its objectives. | | |
| | A disaster recovery policy is shared on the Company intranet and reviewed on an annual basis. | Inspected the disaster recovery policy and Company intranet to determine the disaster recovery policy was reviewed during the period and shared on the Company intranet. | No exceptions noted. |

## Availability

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| | A disaster recovery plan is in place and tested quarterly. | Inspected the disaster recovery plan and tests for a sample of quarters to determine that a disaster recovery plan was in place for all in-scope systems and tested on a quarterly basis. | No exceptions noted. |
| | 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 backup and recover customer data. | No exceptions noted. |
| | System data of products and services is backed up at least daily. Restoration testing occurs annually to ensure data security and integrity is maintained. | Inspected backup configurations to determine that system data of products and services was backed up at least daily. | No exceptions noted. |
| | | Inspected restoration testing documentation to determine that restoration testing was performed during the period to ensure data security and integrity was maintained. | No exceptions noted. |

## Additional Criteria for Confidentiality

| Confidentiality | | | |
|---|---|---|---|
| **TSC Reference** | **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. | | |
| | A data classification policy is in place to support the safety and security of data Atlassian holds. | Inspected the data classification policy to determine that a data classification policy was documented to support the safety and security of data Atlassian holds. | No exceptions noted. |
| | Production data is not used in non-production environments as part of the Software Development Lifecycle Procedures. | Inspected the Software Development Lifecycle Procedures to determine that production data was prohibited by policy from being used in non-production environments. | No exceptions noted. |
| | | Observed the test environment to determine that only test data was used in non-production systems or environments. | No exceptions noted. |
| | Vendor agreements, including any security, availability, and confidentiality commitments, are reviewed during the procurement process for all critical vendors. | Inspected contracts for a sample of critical vendors to determine that vendor agreements, including any security, availability, and confidentiality commitments, were reviewed during the procurement process. | No exceptions noted. |
| **C1.2** | The entity disposes of confidential information to meet the entity's objectives related to confidentiality. | | |
| | Customer data is disposed of, destroyed, or erased upon request in accordance with the retention period or upon termination of services. | Inspected data deletion configurations for in scope products to determine customer data was disposed of, destroyed, or erased upon request in accordance with retention period or upon termination of services. | No exceptions noted. |

| Confidentiality | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | Storage media containing sensitive data and licensed software is removed and securely overwritten prior to disposal. | Inspected certificates of destruction for a sample of purged or destroyed media to determine that storage media containing sensitive data and licensed software was removed and securely overwritten prior to disposal. | 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 |
|---|---|---|
| Employees acknowledge the Code of Business Conduct and Ethics policy upon hire. | Exceptions noted. 1 out of a sample of 44 new employees did not acknowledge the Code of Business Conduct and Ethics policy upon hire. | The relevant team at Atlassian has followed up with the employee who had not signed the Code of Business Conduct and Ethics policy as part of their onboarding process and this was escalated to management for review. The employee who was hired as an intern did not acknowledge the policy before their departure 3 months after their start date. Atlassian HR has established a process for escalation procedures to Legal for incomplete acknowledgements. |