COALFIRE CONTROLS

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

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

ATLASSIAN

Jira Cloud | Confluence Cloud | Bitbucket Cloud | Bitbucket Pipelines | Opsgenie | Forge | Atlas Jira Service Management and Insight | Jira Product Discovery | Data Lake | Atlassian Analytics | Compass

Table of Contents

Section 1

Independent Service Auditor's Report

Independent Service Auditor's Report

To: Atlassian Corporation Plc ("Atlassian")

Scope

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

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

Atlassian uses a subservice organization to provide data center colocation services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Atlassian, to achieve Atlassian's service commitments and system requirements based on the applicable trust services criteria. The description presents Atlassian's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Atlassian's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, 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 Platform made available to user entities during the period October 1, 2021 to September 30, 2022. 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.

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

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

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

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

Inherent Limitations

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

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

Description of Tests of Controls

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

Opinion

In our opinion, in all material respects—

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

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

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

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Atlassian, user entities of the Atlassian Platform during some or all of the period October 1, 2021 to September 30, 2022, business partners of Atlassian subject to risks arising from interactions with the Atlassian Platform, 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, the subservice organization, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.

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

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

Coalfire Controls LLC

Westminster, Colorado
December 8, 2022

Section 2

Assertion of Atlassian Corporation Plc Management

Assertion of Atlassian Corporation Plc ("Atlassian") Management

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

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

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

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

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

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

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

Adrian Ludwig
Chief Trust Officer
Atlassian Corporation Plc

Section 3

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

Type of Services Provided

Company Overview and Background

Atlassian Corporation Plc (“Atlassian”) was founded in 2002 by Scott Farquhar and Mike Cannon-Brookes. Atlassian had its initial public offering (IPO) in 2015.

Atlassian has offices across the globe including the United States (San Francisco, Mountain View, New York City, Austin, Boston), Australia (Sydney), Philippines (Manila), Japan (Yokohama), Netherlands (Amsterdam), Poland (Gdansk), Turkey (Ankara), and India (Bengaluru). Atlassian embraces distributed teamwork, enabling employees to work remotely across Australia, Canada, France, Germany, India, Japan, New Zealand, the Netherlands, the Philippines, the United Kingdom, the United States, and Turkey.

Atlassian's mission is to unleash the potential in every team. Its collaboration software helps teams organize, discuss, and complete shared work. Thousands of teams across large and small organizations worldwide use Atlassian's project tracking, content creation and sharing, real-time communication, and service management products to work better together and deliver quality results on time. Atlassian products include, but not limited to, Jira Suite (Jira and a Jira Work Management [JWM]), Jira Service Management (JSM), Jira Product Discovery (JPD), Confluence, Atlas, Atlassian Analytics, Bitbucket Cloud, Compass, Data Lake, Forge, Insight, Statuspage, Trello, Opsgenie, Jira Align, and Halp.

The systems in-scope for this report are the systems hosted at Amazon Web Services (AWS), and the supporting information technology (IT) infrastructure and business processes. This report does not include on-premise versions (e.g., Jira and Confluence Server and Data Center) or add-ons from the marketplace and open source downloadables added by customers to their instance.

Overview of Products and Services

Jira and Confluence Cloud

Jira and Confluence Cloud covers the Jira Suite (Jira Software and JWM) and Confluence. The Jira family of products is used to manage projects and track issues, with Confluence providing document management and collaboration.

Jira Service Management (JSM) and Insight

JSM is an IT service management (ITSM) solution built on the Jira platform that empowers teams to collaborate, so they can respond to business changes and deliver customer and employee experiences.

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

Jira Product Discovery (JPD)

JPD is a collaborative tool that allows teams to work together on new products.

Atlas

Atlas is a teamwork directory that connects and enables teams to openly communicate and obtain the context they need about their work.

Bitbucket Cloud

Bitbucket Cloud is used to store, manage, and operate in repositories, which are used by customers to track version-controlled changes to software projects.

Bitbucket Pipelines

Bitbucket Cloud offers a built-in additional integrated continuous integration and continuous delivery (CI/CD) service named Bitbucket Pipelines. Bitbucket Pipelines allows for delivery of bug fixes, features, and configuration changes into production through automation of acceptance and integration testing for efficient and reliable deployments.

Compass

Compass is used to track and manage the output of software engineering teams (e.g., libraries, services).

Data Lake

Data Lake is a multi-region data lake for existing Jira customers, designed to enable querying of their own Atlassian product data with business intelligence (BI) tools such as Tableau and eventually integrate with Atlassian Analytics.

Atlassian Analytics

Atlassian Analytics allows teams to query and analyze from their Atlassian data and other third-party data. It's built on top of the Atlassian Data Lake which offers clean, modeled data across Atlassian products and refreshes data for up-to-date access. Teams can leverage pre-built dashboards or create their own from scratch, making use of the customizable visualization options. Atlassian Analytics also has collaboration and sharing features so teams can work together in the context that best suits their needs.

Forge

Forge is a platform for building applications to customize, extend, and integrate with Atlassian Cloud products. Forge provides built-in security, Atlassian-hosted infrastructure, and user interface (UI) extensibility options. It also offers a streamlined DevOps experience with development, staging, and production environments. Forge is currently available for Jira and Confluence Cloud.

Opsgenie

Opsgenie is an incident management platform for operating always-on services, empowering Development and Operations teams to plan for service disruptions and stay in control during incidents. With many deep integrations and a highly flexible rules engine, Opsgenie centralizes alerts, notifies designated people, and enables collaboration for rapid action. Throughout the entire incident lifecycle, Opsgenie tracks all activity and provides actionable insights to improve productivity and drive continuous operational efficiencies.

Principal Service Commitments and System Requirements

Atlassian designs its processes and procedures to meet the objectives of the Atlassian Platform that includes Jira Cloud, Confluence Cloud, Opsgenie, JSM and Insight, JPD, Atlassian Analytics, Atlas, Bitbucket Cloud, Bitbucket Pipelines, Data Lake, Forge, and Compass systems ("the Systems"). Those objectives are based on the service commitments that Atlassian makes to user entities; the laws and regulations that govern the provision of the Systems; and the financial, operational, and compliance requirements that Atlassian has established for the Systems.

Security, availability, and confidentiality commitments to user entities are documented and communicated in the terms of service within the sign-up page in the Systems, the Privacy Policy, and through the Atlassian Trust Security Page. The description of the service offering and the system delineating the boundaries and describing relevant components is documented on the Atlassian intranet and the customer-facing website. The security, availability, and confidentiality commitments include, but are not limited to, the following:

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

Atlassian establishes operational requirements that support the achievement of security, availability, and confidentiality commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Atlassian's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Atlassian Platform.

- Operational Practices – A range of security and confidentiality controls designed to address the security and confidentiality criteria of the Atlassian Platform. Such security and confidentiality controls include permitting system users to access customer data and the information they need based on their roles and responsibilities, while restricting them from accessing information not needed for their role.
- Product Security – A range of security controls Atlassian implements to keep the Atlassian Platform systems and customer's data safe. This includes the use of encryption technologies to protect customer data at rest and in transit and formal processes to grant and revoke access to customer data.
- Reliability and Availability – Hosting data with Atlassian's cloud hosting partners while focusing on product resiliency to minimize downtime. Optimal performance with global redundancy and failover options including maintaining multiple locations and availability zones (AZs) across AWS regions.
- Security Process – A range of vulnerability and security processes to detect security and vulnerability issues, which allows Atlassian to address identified gaps as soon as possible to minimize impact.

The Components of the System Used to Provide the Services

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

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

Infrastructure

Atlassian products are hosted at AWS data centers, using the AWS infrastructure as a service offering (IaaS). The various services making up the runtime and provisioning systems for these products are deployed in multiple AWS regions across the world, for redundancy, high availability, and fault-tolerance, specifically:

Infrastructure								
Product	**AWS Region(s)**							
	Us-east-1	**Us-east-2**	**Us-west-1**	**Us-west-2**	**Eu-central-1**	**Eu-west-1**	**Ap-southeast-1**	**Ap-southeast-2**
Jira and Confluence Cloud (including JWM and JPD)	✓			✓	✓	✓	✓	✓
JSM (including Insight)	✓	✓		✓	✓	✓	✓	✓
Atlas	✓			✓	✓	✓	✓	✓
Atlassian Analytics	✓			✓	✓	✓	✓	✓
Bitbucket Cloud	✓		✓	✓	✓	✓	✓	✓
Bitbucket Pipelines	✓			✓	✓	✓	✓	✓
Compass	✓			✓	✓	✓	✓	✓
Data Lake	✓				✓		✓	✓
Forge				✓				
Opsgenie*		✓		✓	✓	✓		

*Upon sign-up, Opsgenie customers have the option to choose which region (US or EU) to store their data.

Network

Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Atlassian Analytics, and Compass

All network access to the above-mentioned products uses tenant-specific domain name system (DNS) names, such as *tenantname*.atlassian.net (and some *tenantname*.Jira.com legacy records). At all points, the network traffic is encrypted with transport layer security (TLS) 1.2.

All these DNS names resolve to a wildcard record under *.atlassian.net (or *.Jira.com). The DNS response is latency-based (e.g., it will return a set of internet protocol [IP] addresses that are closest to the requestor based on latency).

Atlassian has public ingress points in multiple AWS regions. These traffic manager clusters terminate public TLS and forward the request to proxies hosted in AWS regions. The proxies in AWS look up the physical location (the shard) for the intended tenant, based on the requested hostname, and forward the request to the correct location, which may be in an AWS region other than the one in which the proxy is located. All AWS hosted network traffic is inside the Atlassian Cloud Network, and all traffic in AWS regions, as well as between AWS regions, uses AWS transit gateway or virtual private cloud (VPC) peering.

Bitbucket Cloud and Bitbucket Pipelines

All network access to Bitbucket Cloud and Bitbucket Pipelines uses one of the two DNS records, bitbucket.org or bitbucket.io. At all points, the network traffic is encrypted with at least TLS 1.2.

The DNS response is latency-based (e.g., it will return a set of IP addresses that are closest to the requestor based on latency). Public ingress points are provided by AWS Global Accelerator, which in turn uses Amazon Route53 for geolocation reference.

Data Lake

Direct access to Data Lake is not provided; however, access to data is gained via a customer's chosen BI tool via Cloud API token. Data Lake data is encrypted in transit via HTTPS connection and valid secure sockets layer (SSL) certificates are installed.

Forge

All network access to the developer console uses the DNS record developer.atlassian.com. At all points, the network traffic is encrypted with TLS 1.2.

All other Forge interactions go through api.atlassian.com, which is also encrypted with TLS 1.2.

The DNS response is latency-based (e.g., it will return a set of IP addresses that are closest to the requestor based on latency). Atlassian has public ingress points in multiple Amazon regions. These traffic manager clusters terminate public TLS and forward the request to the API gateway hosted in AWS regions. The API gateway then forwards the request to the correct location, which may be in an AWS region other than the one in which the proxy is located.

Opsgenie

Network access to the web application uses tenant specific DNS names, such as *tenantname*.app.opsgenie.com. At all points, the network traffic is encrypted with TLS 1.2.

Public ingress points are managed similarly to the above primary product description via AWS services and load balancers.

Servers

Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Atlassian Analytics, Bitbucket Cloud, Bitbucket Pipelines, Compass, Data Lake, and Opsgenie

AWS provides IaaS, which runs the Systems. However, the virtual server and operating system configurations are managed by Atlassian. The AWS IaaS for the above-mentioned products spans multiple data centers and regions. The above-mentioned products have separate AWS accounts for their development and production environments.

Forge

The Forge platform is logically separated to isolate application developer resources from the platform itself.

One or more Forge shared accounts run third party code provided by Forge application developers. This code runs on AWS Lambda which is a serverless environment hosted by AWS and doesn't require Atlassian to manage any servers, virtual or otherwise. AWS is in full control of this runtime environment and manages all the associated hardware and operating systems. Code running in Lambda runs in multiple AZs in a single region.

The Forge management code runs on Amazon Elastic Compute Cloud (Amazon EC2) virtual servers provided by AWS. These virtual servers and operating system configurations are managed by Atlassian. The AWS infrastructure for this area spans multiple AZs in multiple regions across the world.

Development of the Forge platform is isolated from the production service with dedicated AWS accounts.

Database

Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Atlassian Analytics, and Compass

The above-mentioned products use logically separate Amazon Relational Database Service (Amazon RDS) databases for each product instance (e.g., tenant data is separated at the database level). Multiple databases may share the same database server that is hosted by AWS, each having an independent synchronous replica in a different AZ within the same AWS region to mitigate the risk of data loss due to hardware failure.

Backups are kept for 30 days as redundancy to allow point-in-time recovery (PITR) of data.

All attachments are stored in the document storage platform (Media Platform), and all other data is stored in Amazon Simple Storage Service (Amazon S3) for increased durability and segregated by tenant using a unique identifier that is stored in the product database. The unique identifier is stored in an Amazon DynamoDB (DDB), which relates the customer to its respective data store.

Amazon S3 is used as a file service for user attachments, backups, and log archives. Amazon S3 is fully managed by AWS. S3 provides durability and availability and is the responsibility of AWS.

Bitbucket Cloud

Bitbucket Cloud uses a single shared Amazon Aurora database for all customers. The database server has multiple independent synchronous replicas in multiple AZs within the same AWS region to mitigate the risk of data loss due to hardware failure. Backups are kept for 30 days as redundancy to allow restoration of data within a reasonable point in time, if needed.

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

Amazon S3 is used as a file service for user attachments, backups, and log archives. Amazon S3 is fully managed by AWS. Amazon S3 provides durability and availability and is the responsibility of AWS.

Bitbucket Pipelines

Bitbucket Pipelines' primary data storage utilizes DDB, which is hosted by AWS and managed by Atlassian. DDB is highly available, scalable, and spans multiple data centers and regions. Amazon Elasticsearch Service (Elasticsearch) is used to index DDB tables using a custom *indexer sidecar*, which listens on each DDB's table stream endpoint for all modifications to items and updates Elasticsearch documents to continually reindex for querying purposes. Redis is additionally used in some services for distributed locking, caching, and managing commit responses for in-line code annotations.

Compass

Compass uses Phi Graph Store (PGS) which is based on DDB and Elasticsearch.

DDB is used as a primary store, with Elasticsearch as secondary indexing, allowing for more flexible queries. Elasticsearch data can be considered ephemeral as it can be reindexed from the primary copy in DDB.

Data Lake

All Data Lake data is stored in Amazon S3 and is encrypted in transit and at rest. Views will be created for customers in their own namespace/schema, utilizing shard filtering over the base refined tables to optimize reads on the refined tables. Customers can only query tables and views in their own namespace, using table access control lists (ACLs) to prevent cross-contamination and restrict visibility of data.

Forge

Forge application metadata is stored in multiple Amazon RDS databases, each having an independent synchronous replica in a different AZ within the same AWS region to mitigate the risk of data loss due to hardware failure. Backups are kept for 30 days as redundancy to allow PITR of data. Amazon S3 is used to store backups and log archives, providing high durability and availability and is the operational responsibility of AWS.

A copy of application metadata is stored in DDB to provide fast read operations. The application artifacts are kept in Amazon S3 and are logically separated from other customer data in dedicated AWS accounts with separate credentials.

Forge applications may store application data with the Forge storage API, providing a key value datastore backed by DDB.

Opsgenie

Opsgenie's primary datastore is DDB, which is hosted by AWS and managed by Opsgenie. DDB is highly available, scalable, and spans multiple data centers and regions. Opsgenie uses Global Tables (AWS) spanning multiple regions offering high availability by AWS. Zone based failures and data corruption are automatically recovered by AWS.

Elasticsearch is used as a text search engine. It is managed by the Opsgenie team and hosted within the AWS private network, spanning multiple data centers and regions.

Amazon S3 is used as a file service for user attachments, backups, and log archives. Amazon S3 is fully managed by AWS. Amazon S3 provides durability and availability and is the responsibility of AWS.

Provisioning Architecture

Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Atlassian Analytics, Bitbucket Cloud, Bitbucket Pipelines, Compass, Data Lake, Forge, and Opsgenie

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

In addition, for Forge, a user account is created and provided to the customer to access the application.

Software

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

Software		
Function	**Description**	**Component(s)**
Hosting Systems	Amazon EC2	Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Atlassian Analytics, Bitbucket Cloud, Bitbucket Pipelines, Compass, Data Lake, Forge, and Opsgenie
	Kubernetes on top of Amazon EC2	JSM and Insight and Bitbucket Pipelines
	CentOS	Compass
	Lambda	Forge
Storage and Database	Amazon RDS for PostgreSQL	Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Atlassian Analytics, Compass, and Forge
	DDB	Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Bitbucket Cloud, Bitbucket Pipelines, Compass, Forge, and Opsgenie
	Amazon S3	Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlassian Analytics, Bitbucket Cloud, Bitbucket Pipelines, Compass , Data Lake, Forge, and Opsgenie
	Aurora	Bitbucket Cloud, Forge, and Opsgenie
	AWS Key Management Service (AWS KMS)	Opsgenie

Software		
Function	**Description**	**Component(s)**
	NetApp cloud volume service (CVS)	Bitbucket Cloud
	Redis	Atlas, Bitbucket Pipelines, Forge, and Opsgenie
	Databricks Workspaces	Data Lake
Network	Amazon virtual private cloud (VPC)	Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Atlassian Analytics, Bitbucket Cloud, Bitbucket Pipelines, Compass, Data Lake, Forge, and Opsgenie
	Amazon Load Balancers (ALB)	Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Atlassian Analytics, Bitbucket Cloud, Bitbucket Pipelines, Compass, Data Lake, Forge, and Opsgenie
	Corporate firewall	Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Atlassian Analytics, Bitbucket Cloud, Bitbucket Pipelines, Compass, Data Lake, Forge, and Opsgenie
	Amazon CloudFront	Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Atlassian Analytics, Bitbucket Cloud, Bitbucket Pipelines, Compass, Data Lake, Forge, and Opsgenie
	Amazon Web Application Firewall (WAF)	Forge, JSM and Insight, and Opsgenie
	Kubernetes	Opsgenie
Application Cache	Amazon ElastiCache	Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlassian Analytics, Bitbucket Cloud, Compass
	Redis	Atlas, Bitbucket Pipelines, Forge, and Opsgenie
Search and Analytics	Elasticsearch	Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Atlassian Analytics, Bitbucket Cloud, Bitbucket Pipelines, Compass, Data Lake, Forge, and Opsgenie
Messaging	Amazon Simple Queue Service (Amazon SQS)	Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Atlassian Analytics, Bitbucket Cloud, Compass, Data Lake, Forge, and Opsgenie
	Kinesis	Forge and Opsgenie
	Amazon Simple Notification Service (Amazon SNS)	Bitbucket Pipelines and Opsgenie

Software		
Function	**Description**	**Component(s)**
Build, Release, and Continuous Integration Systems	Deployment Bamboo	Jira Cloud, Confluence Cloud, JSM and Insight, JPD
	Bitbucket Cloud	Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Atlassian Analytics, Bitbucket Cloud, Compass, Data Lake, Forge, and Opsgenie
	Bitbucket Pipelines	Atlassian Analytics, Atlas, Bitbucket Cloud, Bitbucket Pipelines, Compass, Data Lake, Forge, and JSM and Insight
Access Management	Active Directory	Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Atlassian Analytics, Bitbucket Cloud, Bitbucket Pipelines, Compass, Data Lake, Forge, and Opsgenie
	CyberArk (formerly Idaptive) single sign on (SSO)	Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Atlassian Analytics, Bitbucket Cloud, Bitbucket Pipelines, Compass, Data Lake, Forge, and Opsgenie
	Duo two-factor authentication (2FA)	Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Atlassian Analytics, Bitbucket Cloud, Bitbucket Pipelines, Compass, Data Lake, Forge, and Opsgenie
Monitoring and Alerting	New Relic	Bitbucket Cloud and Opsgenie
	Opsgenie	Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Atlassian Analytics, Bitbucket Cloud, Bitbucket Pipelines, Compass, Data Lake, Forge, and Opsgenie
	SignalFX	Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Atlassian Analytics, Bitbucket Cloud, Bitbucket Pipelines, Compass, Data Lake, Forge, and Opsgenie
	Splunk	Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Atlassian Analytics, Bitbucket Cloud, Bitbucket Pipelines, Compass, Data Lake, Forge, and Opsgenie
Customer Support and Communication	Atlassian Community	Data Lake
	Intercom	Opsgenie
	Statuspage	Jira Cloud, Confluence Cloud, JSM and Insight, Bitbucket Cloud, Bitbucket Pipelines, Compass, Forge, and Opsgenie

Software		
Function	**Description**	**Component(s)**
Vulnerability Scanning	Cloud Conformity	Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Atlassian Analytics, Bitbucket Cloud, Bitbucket Pipelines, Compass, Data Lake, Forge, and Opsgenie
	Nexpose	Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Atlassian Analytics, Bitbucket Cloud, Bitbucket Pipelines, Compass, Data Lake, Forge, and Opsgenie
	Snyk	Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Atlassian Analytics, Bitbucket Cloud, Bitbucket Pipelines, Compass, Data Lake, Forge, and Opsgenie
	SourceClear	Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Atlassian Analytics, Bitbucket Cloud, Bitbucket Pipelines, Compass, Data Lake, Forge, and Opsgenie
Human Resource	Workday	Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Atlassian Analytics, Bitbucket Cloud, Bitbucket Pipelines, Compass, Data Lake, Forge, and Opsgenie
	Lever	Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Atlassian Analytics, Bitbucket Cloud, Bitbucket Pipelines, Compass, Data Lake, Forge, and Opsgenie
Notifications	Nexmo	Opsgenie
	Mailgun	Opsgenie
	Twilio	Opsgenie
	Pubnub	Opsgenie

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

People

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

People	
Group/Role Name	**Function**
Co-Founders and Executive Management	Responsible for overseeing company-wide activities, establishing and accomplishing goals, and managing objectives.
Engineering	Responsible for the development, testing, deployment, and maintenance of new code for the Atlassian Platform
Trust	Responsible for managing access controls and the security of the production environment.
Product Management	Responsible for overseeing the product life cycle, including adding new product functionality.
People (in partnership with the people leaders)	Responsible for determining the right talent strategy to deliver against the needs of Atlassian. The People team is responsible for talent acquisition and learning, total rewards and technology, and workplace experiences.
Platform and Enterprise Cloud	Responsible for validating the demands of customers and providing insight and guidance around minimum viable product and user experience.
Foundation	Responsible for harnessing the resources of Atlassian to champion organizations who believe that education is the key to eliminating disadvantage. This is accomplished by improving educational outcomes in developing countries, increasing skill-based volunteering, and leveraging Atlassian's products.
Legal	Responsible for matters related to corporate development, privacy, general counsel operations, and public relations.
Finance	Responsible for handling finance and accounting.
Chief Technology Officer (Technology Operations)	Responsible for overseeing the Engineering, Trust, Risk and Compliance, Information Security, Mobile, Ecosystem, and Platform teams.

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

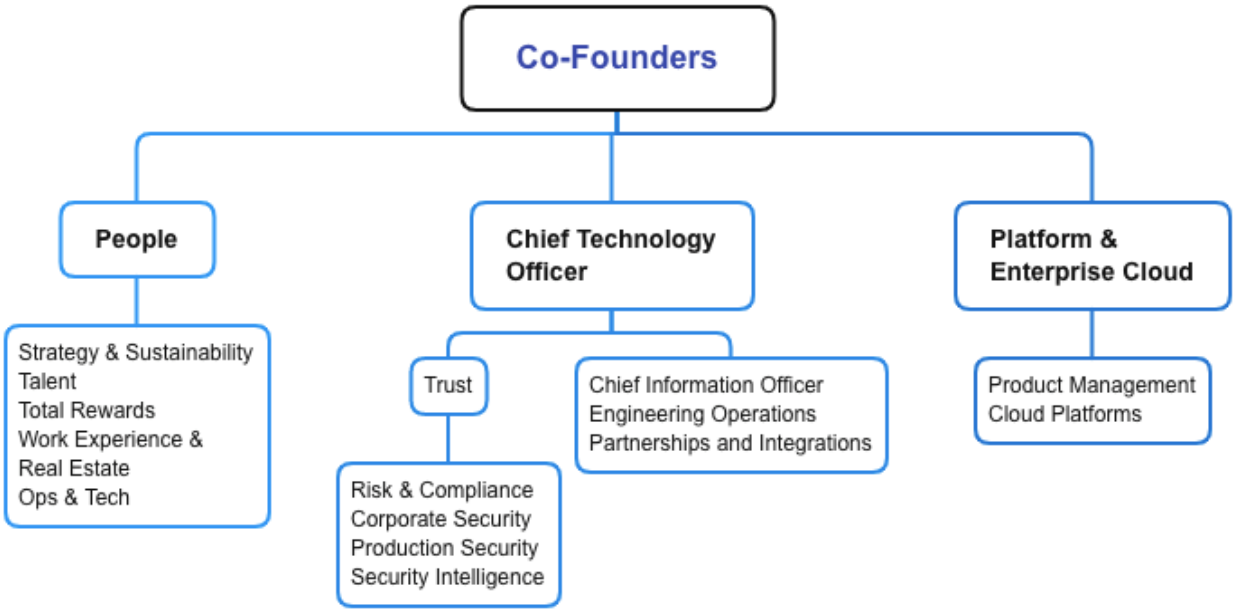

Figure 1: Atlassian Platform Organization Chart

Policies and Procedures

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

- properly communicated throughout the organization
- properly owned, managed, and supported
- clearly outlining business objectives
- showing commitment to meeting regulatory obligations
- focused on continual iteration and improvement
- provided for an exception process
- supported by the Policy Framework and Structure

Atlassian defines policies, standards, guidelines, and procedures, and each document maintained by Atlassian is classified into one of these four categories based on the content of the document.

Policies, Standards, Guidelines, and Procedures		
Item	**Defines**	**Explanation**
Policy	General rules and requirements	Outlines specific requirements or rules that must be met.
Standard	Specific details	Collection of system-specific or procedural-specific requirements that must be met by all employees.

Policies, Standards, Guidelines, and Procedures		
Item	**Defines**	**Explanation**
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 and Guideline requirements, in accordance with the rules	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 or procedure is to help achieve a consistent outcome as 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 team. Policy Owners can approve exceptions for a period no longer than one year.

Policy Review Process

To advance a policy, standard, guideline, or standard operating procedure to be available internally to all Atlassian employees, each document will go through a review process. The review process follows Atlassian’s internal process where feedback is sought from a small group of knowledgeable peers on the topic. After feedback is incorporated, the draft document is submitted to the Policy Committee, either via email or via the internal corporate chat system. Any updates to policies, standards, or guidelines are shared via email and the internal website where all policies are stored.

Data

Customers sign up for an Atlassian account on https://www.atlassian.com/. Upon completing the sign-up process, a new database record and unique identifier is created in the database for that customer account and their organization. The unique ID is used thereafter for associating data with the specific organization. The data is logically separated from other users and organizations’ data using these unique IDs. All user-created data are similarly assigned unique identifiers such that those identifiers can be correctly associated to users and organizations.

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

System Incidents

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

The Applicable Trust Services Criteria and Related Controls

Applicable Trust Services Criteria

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

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

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

The common criteria are organized as follows:

1. *Control environment:* The criteria relevant to how the entity is structured and the processes the entity has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values, qualifications of personnel, and the environment in which they function.
2. *Communication and information:* The criteria relevant to how the entity communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.
3. *Risk assessment:* The criteria relevant to how the entity (i) identifies potential risks that would affect the entity’s ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.
4. *Monitoring activities:* The criteria relevant to how the entity monitors the system, including the suitability and design and operating effectiveness of the controls, and acts to address deficiencies identified.

5. *Control activities:* The criteria relevant to the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out.
6. *Logical and physical access controls:* The criteria relevant to how the entity restricts logical and physical access, provides and removes that access, and prevents unauthorized access.
7. *System operations:* The criteria relevant to how the entity manages the operation of system(s) and detects and mitigates processing deviations, including logical and physical security deviations.
8. *Change management:* The criteria relevant to how the entity identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
9. *Risk mitigation:* The criteria relevant to how the entity identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

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

Control Environment

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

Integrity, Ethical Values, and Competence

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

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

Learning and Development

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

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

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

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

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

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

The audit committee charter is published on Atlassian’s Investor’s website under Governance Documents. The audit committee charter includes roles, responsibilities, key activities, and meetings. Qualifications for the audit committee’s Financial Expert role are also outlined and defined within the audit committee charter. The audit committee meeting calendar and meeting agenda are developed. The audit committee meeting is published annually. Results of the audit committee meeting are published after the meeting has completed. The agenda includes items to be discussed and general questions and answers about the annual general meeting, such as who is allowed to vote at the annual general meeting.

Organizational Structure

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

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

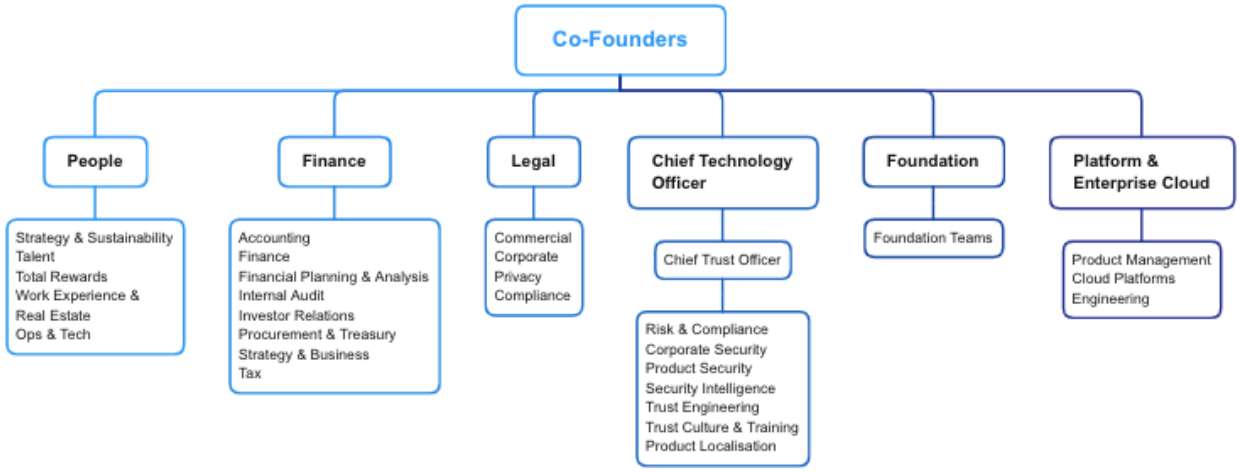

Figure 2: Atlassian's Organizational Chart

The organizational charts are reviewed by appropriate Atlassian management and updated semi-annually. Additionally, organizational charts are automatically updated based on employee action notices and are available to all Atlassian employees via Atlassian's HR system, Workday.

The co-founders are responsible for directing all designated areas including Platform and Enterprise Cloud, People, Foundation, Legal, Finance, and the Technology teams. All teams have full responsibility over key operations within Atlassian. Refer to the People table above for more detail regarding the functions of each team.

Management's Philosophy and Operating Style

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

- Standards — Atlassian follows specific standards that enable the organization to exercise practices around security, availability, quality, reliability, and confidentiality.
- Tools — Atlassian leverages tools designed specifically to assist in identifying, analyzing, tracking, deciding, implementing, and monitoring risks and findings. In addition, the tools allow the Company to effectively communicate and collaborate using workflows to help ensure that activities are properly tracked. The use of customized tools allows them to be more closely integrated with the standard way of how Atlassian operates: specific, scalable, systematic, and robust.
- Enterprise Risk Management Process — Atlassian uses an Enterprise Risk Management process that is modeled after ISO 31000:2009 Risk Management — Principles and Guidelines.
- Unified Approach — As Atlassian becomes involved across various best practices, legal, and regulatory requirements, it becomes more essential to create control activities that are universal and not unique to specific standards and guidelines. Instead of tracking control activities specific to a standard, Atlassian tracks activities that are universal and meet multiple standards. This approach has enabled Atlassian to speak a common language across the organization. Along with a unified approach comes operational efficiency and a way to establish a controlled environment more effectively.

Human Resources Policies and Procedures

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

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

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

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

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

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

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

Communication and Information

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

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

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

Atlassian uses the Atlassian Trust Center website to communicate the latest information on the security, reliability, confidentiality, and compliance of its products and services. This includes communicating its membership to the Cloud Security Alliance and providing information on its compliance program and the various control standards it adheres to, such as ISO27001.

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

- Customer Support - https://support.atlassian.com/ is the service desk where customers can submit requests for support from Atlassian. Customer issues are handled by Atlassian Support and escalated to engineering teams if needed.
- Developer Community - https://community.developer.atlassian.com/ is the community where developers ask questions and communicate with other developers and Atlassian in a public forum.
- Ecosystem Support - https://ecosystem.atlassian.net/servicedesk/customer/portal/14
- Opsgenie Support - https://www.opsgenie.com/contact-us
- Social media
- General website forums
- Email
- Public bug sites

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

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

Atlassian. The availability of the Systems, including the status and uptime, is published in the customer-facing website for all customers.

Risk Assessment and Mitigation

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

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

The ERM process is modeled after ISO 31000-2009 Risk Management — Principles and Guidelines.

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

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

- Business goals and objectives — High level business goals and objectives, and the strategies in place to achieve these goals and objectives.
- Major initiatives — Large projects and initiatives that could have a significant impact on the Company's risk profile. Additionally, Risk and Compliance managers are engaged by various teams, and they bring their knowledge of the environment into consideration.
- Risk and Compliance assessments — Throughout the year, Atlassian performs several periodic and ad-hoc assessments, which include key product stakeholders. Results of the assessments are captured in the Atlassian Governance, Risk, and Compliance (GRC) tool.
- Incidents — Atlassian utilizes a common Incident Management (IM) process, including Post Incident Review (PIR). The goal of PIR is not only to establish the root cause but also to create actions aimed at reducing the risk of repeated incidents.
- Organizational policies — Organizational policies that have been put in place to achieve the organization’s strategic goals and objectives.
- Interviews with major stakeholders and subject matter experts (SMEs) — As part of the structured enterprise risk assessment, Atlassian interviews all members of the Management team and engages with SMEs as needed.
- Other sources — Atlassian may consult industry publications, analyses, and incidents, as necessary.

Internal and external context of the ERM process includes but is not limited to understanding:

- Competitive environment — Who are Atlassian's major competitors, what threat level they present, and what are the trends in Atlassian's industry
- Legal and regulatory environment — What are Atlassian's obligations within their operating jurisdictions, and what are the industry standards Atlassian needs to abide by
- Financial environment — Status as well as trends in the financial and currency markets that could affect Atlassian, perceptions of the Company, and values of external stakeholders
- Technological environment — What are the trends in technology and software development
- Business environment — Markets that Atlassian is currently in or plans to enter; the perception of Atlassian and its products and services; and what are the current developments and trends in Atlassian's ecosystem, major vendors, and customers
- Human environment — What are the social and cultural trends that could affect Atlassian, and what are the status and trends of the talent pools where Atlassian currently has or plans to establish a presence
- Natural environment — Considerations related to natural disasters and office locations and facilities

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

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

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

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

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

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

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

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

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

Entity Level Risk

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

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

Vendor Management

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

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

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

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

Information Security

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

Information Security Controls

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

Periodic Review of Risks and Controls

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

Information Security Training

Appropriate training enables employees to comply with their responsibilities as they relate to the Information Security Policy.

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

Disciplinary Notice

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

Monitoring

The Product Operations and Engineering teams monitor a wide variety of metrics across the services to maintain and improve users' experience. Status of the Systems is published online together with details of historical incidents that have impacted availability.

The Systems utilize an internal Platform as a Service (PaaS) and monitoring platforms, which provide monitoring of application metrics, including AWS dependencies. The various monitoring tools include:

- Data aggregation for measuring availability and reliability
- Health of the application via throughput and potential errors within the application
- Endpoint health checks
- System log patterns

Automated alerts are configured to notify members of the Cloud Operations team based on a rotating pager schedule when certain thresholds for service metrics are crossed, so that immediate action can be taken following the Incident Management process.

Technical Vulnerability Management

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

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

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

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

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

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

Penetration Testing

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

Endpoint Protection and Asset Management

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

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

Email Scanning

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

ZeroTrust Network

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

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

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

Encryption

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

Internal and External Audit

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

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

Control Activities

Logical Access

Customer Production Accounts: Provisioning

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

Atlassian also has agreements between Solution Partners and Global Alliance Partners (Partners), in which Partners can join a program to resell Atlassian's offerings. For customers who purchase directly through a Partner, their access to and use of the offerings is subject to the applicable customer agreement. Partners are responsible for ensuring that each customer has entered into the customer agreement, at or before such customer’s purchase or use of the offerings, in a manner that is legally binding upon the customer.

From time to time, based on proposed deal size, the Atlassian legal department may negotiate a master services agreement with certain enterprise customers.

There is no production data residing in the non-production environments of the Systems and complies with the confidentiality requirements based on the region in which customers select.

Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Atlassian Analytics, Compass, and Data Lake

After acknowledging the customer agreement, the customer's order is accepted and provisioned. Dedicated databases for the customer product instances are created in Amazon RDS. Each customer's database is logically separated from other customers' databases, and the provisioning systems prevent one database being assigned to multiple customers. Unique identifiers are assigned to customers upon creation, which logically segregate data from other accounts. The customer can then start using the systems noted, as well as the associated databases. After successful provisioning, the customer's configuration information is stored in the Catalogue Service (CS). The CS stores the master copy of the customers' configuration information (e.g., database location), which is then fed into the Tenant Context Service (TCS) for access at runtime. The identity details of the site administrator and any users they create are kept in a dedicated Atlassian identity platform, which manages the storage and security of this data, and which provides interfaces for login, authentication, authorization, and session management. For performance reasons, user information is synchronized to the product databases.

Opsgenie

Upon accepting the terms and conditions and completing the sign-up flow, a new database record and unique identifier are created in DDB for that customer account. The unique ID is used thereafter for associating data with the specific customer account. The data is logically separated from other customers' data using these unique IDs. All users in an account have similarly unique IDs for data segmentation. All user created data are also assigned unique identifiers such that they can be correctly associated to users, teams, and accounts.

Bitbucket Cloud and Bitbucket Pipelines

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

Forge

After the customer acknowledges the customer agreement, the customer's user account is created for Forge access. After successful provisioning, the customer's configuration information is stored in the CS. CS stores the master copy of customer configuration information such as database location, which is then fed into the TCS for access at runtime. Each customer database is logically separated from other customers' databases, and the provisioning systems prevent one database from being assigned to multiple customers. Unique identifiers are assigned to customers upon creation, logically separating data from other accounts.

Compass

Compass utilizes Phi Graph Store to store data from multiple customers in the shared tables in DDB. Tenant isolation is at the application layer (e.g., relevant tenant id is a mandatory request parameter). The same applies to Elasticsearch data, which is using shared indexes to store data from multiple customers.

Customer Production Accounts: De-provisioning

Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Atlassian Analytics, Compass, Data Lake, and Forge

Upon termination of service, customer accounts are deactivated within 15 days (for monthly subscriptions) and 17 days (for annual subscriptions) after the end of the customer's current subscription period. Atlassian retains data for deactivated products for 15 days (for evaluation licenses) or 60 days (for Free, Standard, and Premium product plans) after the end of the customer's current subscription period. Upon deletion, an archive of the data is kept for an additional 30 days.

Opsgenie

Customers can view and delete their data via the Opsgenie web application. Once the user or account owner confirms termination of service, the user and account owner's data from the Opsgenie account services will be deleted within 30 days.

When the customer requests to terminate their services via their Opsgenie customer account, a two-day grace period is automatically initiated before the full deletion of their account. Once the two-day period has passed, the deletion of the customer's account is automatically triggered, which includes all data within their account. Engineering has crafted a set of tools to perform the deletion automatically.

Bitbucket Cloud and Bitbucket Pipelines

Upon termination of service, customer accounts are deactivated 15 days after the end of the customer's current subscription period. Upon deletion, an archive of the data is kept for an additional 30 days. Bitbucket Pipelines customer data is deleted when a customer deletes their repository or account within Bitbucket.

Production Environment Access

Customer Access

External users can register for an Atlassian account using an email address and password. Customers are responsible for managing access to their own products and instances. Users with an administrator role within the instance can add and remove user accounts. Users can only access instances they are authorized to.

Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Atlassian Analytics, and Compass

A typical request to the above-mentioned applications connects via HTTPS to the Cloud Smart Edge (CSE), which is a cluster of load balancers closest to the user. The CSE looks up the TCS using the hostname of the request, which stores location information where the request for these applications needs to be routed to. It then forwards the request to the appropriate application cluster. The applications also contact the TCS to determine configuration information for the request, such as the database location and licensing information. The application validates the login session for the user and responds to the request. If the session is not present or not valid, the user is redirected back to the original login system. During the login process, the application verifies whether the user is authorized to access the requested products. If verification passes, a valid session is created, and the user is routed to the requested products. For users who are not authorized, the request is denied. Mobile applications access the applications' APIs via the same path as the other requests. Other ways in which requests can be made to the application clusters is via asynchronous jobs (e.g., an application request that is not directly related to the response to the user such as sending email or running a scheduled job).

Bitbucket Cloud and Bitbucket Pipelines

Access is gained via a typical HTTPS connection, which then routes the request to the proper microservice where the application then validates the login session for the user and responds to the request. Mobile applications access the application and APIs via the same path as other requests. Additional requests can be made to the application clusters via asynchronous jobs (e.g., an application request that is not directly related to the response to the user such as sending email or running a scheduled job) as well as SSH connectivity. SSH connections are terminated directly at the application endpoint.

Data Lake

Customer access is not direct but leverages a Cloud API token through the customer's chosen BI tool. This token is verified to be associated with the correct permissions for the Atlassian organization, and then is translated into that customer identity that is used to control access at the database layer.

Forge - Developer

External users can register for an Atlassian account using an email address and password. Any user with an Atlassian account can create a limited number of applications within the Forge Developer platform.

If developing on the Atlassian platform, the user is directed to acknowledge the standardized Atlassian Developer Terms, which define the developer's responsibility around security, availability, and confidentiality. An application cannot be developed on the Atlassian platform without first being directed to acknowledge the Atlassian Developer Terms. Any updates to the Atlassian Developer Terms are reviewed and approved by the Legal department. Atlassian reserves the right to terminate access to the developer platform if it is deemed necessary (e.g., violation of developer terms, causing platform instability).

Forge - Developed Application User

Administrators of Atlassian products (e.g., Jira, Confluence) can choose to install a Forge Developed Application by granting that application consent and letting it operate in their product. Once installed in a product, a bot account for the application is provisioned that allows the application to act as itself. The bot account is ignored for licensing purposes. The application can also act as a user of that product to provide the intended functionality. Product specific logs cannot be accessed by the application bot accounts.

Opsgenie

Users can access Opsgenie via the browser user interface and mobile applications. Customers can also leverage Opsgenie's REST API by using API keys. Customer-side administrators can create multiple teams in their Opsgenie account. Teams can have members, users, or administrators. Team administrators can authorize users in the account to be a member of a team. Members of a team can only manage configuration and alerts of their teams. Customer account level user roles can override team-based segmentation. Account administrators or custom roles can be configured to manage all team configurations.

Atlassian Internal Users Access

Access to the Systems' production environment is tightly restricted and is provisioned based on the principle of least privilege. Privileged access to production environments is restricted to authorized and appropriate Atlassian users only.

Atlassian access to the underlying AWS accounts, and the corresponding instances providing the Systems' datastore, queues, and supporting tools, are restricted to the members of the Development team. Access can only be gained from within the Atlassian network or while connected to the corporate VPN and requires two-factor authentication via Duo. Additionally, Atlassian users must connect to a jump box and must have a valid key to gain SSH access.

All services are hosted within the production AWS account. Changes to infrastructure and patches are automated, peer reviewed, and tested. In emergency cases, direct access to infrastructure may be used.

Password

Customer Access

Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Atlassian Analytics, Bitbucket Cloud, Bitbucket Pipelines, Compass, Data Lake, and Forge

The password settings for customers are governed through password complexity, in which lowercase, uppercase, numbers, and symbols are used. The default password policy for external users requires a minimum of 8 characters with no hard expiry. It is the customer's responsibility to ensure that their accounts are appropriately configured and set up to their corporate network, password, and other authentication mechanisms such as SSO or two-factor authentication.

Opsgenie

Opsgenie customers are governed with a trial account when they first sign up. It is the customer's responsibility to ensure that their accounts are appropriately configured with SSO, Google Auth, or strong password policies. SSO can be enabled for every user in the account. Strong password policies can enforce a minimum of 8 characters, complex password, password expiration, and prevention of the same password being reused.

Atlassian Internal Users Access

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

Atlassian provides various secure methods to connect to Atlassian resources. The primary method for connecting to Atlassian resources is via the Idaptive SSO system, which requires two-factor authentication. Duo two-factor authentication is also required when logging into the VPN. The only exception is certain IP addresses that are whitelisted within the exempt IP settings in Idaptive. For Atlassian employees, a minimum of 12 characters is enforced for passwords in Idaptive as configured in Atlassian's Active Directory.

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

Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Atlassian Analytics, Bitbucket Cloud, Bitbucket Pipelines, Compass, Data Lake, Forge, and Opsgenie

Active Directory 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, a staff member's assigned groups will be updated to reflect a team or department change or termination. Active Directory group membership is automatically assigned based on the user's department and team.

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

- Each Atlassian user account must have an Active Directory account
- Each Atlassian user account must be a member of the appropriate lightweight directory access protocol (LDAP) group

Access to the AWS production environment, RDS databases, and supporting tools, in addition to the Workday group access, is provisioned only after appropriate approval via a Jira ticket. NetApp, which contains all relevant customer repositories, is provisioned by the Bitbucket Cloud Operations team. Access is based on membership to the appropriate security groups.

Atlassian Internal User De-provisioning

Deprovisioning of access via terminations is initiated at the Workday level. HR initiates the termination once notified by management via Workday. The system does not permit termination dates to be backdated. Idaptive is configured to pull all the upcoming terminations from Workday via a job and then schedules the user to be terminated accordingly in Active Directory (within 8 hours). Once terminated via the above process, users are unable to manually connect to the network, login to the Wi-Fi, or access via VPN, including remote access via Duo and access to the Systems. Additionally, any access to systems that are not managed via Active Directory is manually revoked.

Atlassian Internal User Role Changes

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

Atlassian Internal User Access Reviews

Atlassian's Engineering Managers or team leads perform semi-annual privileged user access reviews on the Systems and the associated in-scope supporting tools and services. Any discrepancies identified are escalated to the respective managers and are addressed in a timely manner based on the nature of remediation required. Privileged access to Workday is limited to appropriate users. The People Central Systems Support Specialist performs a review of Workday administrator users on a semi-annual basis.

Access of Atlassian Support Team to User Data

Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Atlassian Analytics, Bitbucket Cloud, Bitbucket Pipelines, Compass, Data Lake, and Forge

Atlassian has a dedicated group of customer support personnel (Customer Support and Success [CSS]) who help customers troubleshoot issues while using the above-mentioned products. CSS personnel can access customer's instances for a defined temporary period when there is a corresponding open support ticket associated with the customer's account. Access is automatically revoked once the defined duration expires. The CSS team uses the Governator tool to provision temporary access to customer's instances. Access to Governator is formally requested and approved and is reviewed semi-annually.

Opsgenie

Opsgenie has a dedicated group of customer support personnel who help users troubleshoot issues. When a support request is received from a customer, Customer Support with administrator access must raise a consent request using the customer URL from the Opsgenie administrator panel. Customer Support can define the consent duration required for access. The maximum amount of time for access is seven days. The customer must then approve the consent request through their Opsgenie customer account. Once approved, the approval is logged in a corresponding support request ticket, and Customer Support can access the customer's instance. Access is automatically revoked once the approved duration expires. Customers also can withdraw the consent approval before the given consent duration expiry.

Hosting Facilities

Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Atlassian Analytics, Bitbucket Cloud, Bitbucket Pipelines, Compass, Data Lake, Forge, and Opsgenie

The above-mentioned products are hosted within AWS facilities. Atlassian reviews the AWS SOC 2 report on an annual basis to assess the adequacy of the vendor's controls in meeting Atlassian's security, availability, and confidentiality commitments. Any issues identified as part of the review are followed up and addressed as necessary.

System Operations

Incident Management

A Company-wide incident management process is in place. The incident management process must meet the Atlassian Incident Management Standard.

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

The standard principles of incident management consist of the following:

- Detection and Recording — Atlassian has the appropriate tools in place to properly detect and record all incidents.
- Incident Classification for Resolution and Communication — Incidents are classified according to the level of severity. Incident Managers play a crucial part in exercising judgment on the incident priority.
- Communication Steps Based on Severity — The severity of the incident determines the communication steps all Incident Managers take.
- Investigation and Diagnosis — Investigations begin with existing runbooks and other relevant documentation. Many incidents have pre-formulated solutions captured in runbooks.
- Resolution and Recovery — The Incident Management team encourages quick and responsive incident resolution and can resolve incidents immediately.
- Incident Handover — When incidents are escalated and run longer, incident handovers are coordinated.
- Closure and Post Incident Review — Clients and customers can provide feedback on the resolution of the incident. Customer Support or Customer Advocacy confirm the resolution of all customer-reported incidents with the reporting customer. When the incident is completely resolved, the Incident Manager completes and closes all incident records and tickets. After high severity incidents, the Incident Manager completes a PIR, which is to be documented. If the root cause is fully understood from a previous incident, then the PIR can link to that previous incident.
- Incident Reporting and Analysis — Data from IT incidents, including both those received and resolved by Customer Support are typically analyzed and reported for trends and indications of unidentified problems requiring definition and resolution.
- Relation to Problem Management — Where possible, all related or similar incidents are examined for a common cause. Where incidents temporarily cannot be associated with any root cause (problem), they are reviewed for any other common incidents.

The table below describes the severity levels of incidents.

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

Factors considered when determining severity:

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

Change Management

Change Initiation

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

Change Development

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

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

Atlassian uses the merge checks feature built into Bitbucket Cloud to enforce peer review(s) and approval(s) and automated tests (green build tests) before the code can be merged. A green build (successful build) occurs when all the automated tests as defined within the Deployment Bamboo build plan have successfully completed. A red build occurs if any tests defined within the Bamboo build plan fail.

Before a pull request can be merged to the master branch, it must be approved by at least one authorized reviewer. Bitbucket Cloud prevents pull requests from being approved by the same user who requests it. This prevents any direct changes to the master branch except through a peer-reviewed pull request that has undergone successful testing.

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

An Atlassian-only Compliance setting in Bitbucket Cloud prevents any of the above controls from being changed or turned off. If the Compliance setting itself is turned off for a repository, Bitbucket Cloud logs an event to the Atlassian data warehouse, where it triggers an automated alert in the REPCOM system. The alerts are routed to the relevant development manager to confirm that no unauthorized changes were made and to restore the setting. Turning off the Compliance setting may be necessary when implementing emergency changes.

Change Deployment

After a pull request is merged into the production branch and the team is ready to deploy the new version, the deployment is executed via the authorized build systems.

Before a build can be created, the build systems perform a check to confirm that the appropriate configuration settings (e.g., requires successful testing) controls as described above were in effect on the source code repository. If it identifies that the controls are not implemented, it automatically prevents the builds from being deployed.

Only artifacts built by the authorized build system can be deployed to the Systems' production environment. Any artifact deployed by another source is automatically rejected. Only appropriate users that are not developers are given access to the build systems. Additionally, access is reviewed on a semi-annual basis.

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

Scanning of Production Code

The Systems utilize Snyk and SourceClear to continuously scan and review the code base to detect vulnerable open-source libraries being used. The scanners are integrated into the build plan and are run automatically when changes are made to the code base within the Bitbucket Cloud master branch. Jira tickets are then automatically created for high and critical severity vulnerabilities. Developers and Product Security review the reports, assess the vulnerabilities, determine the risk and severity level, and triage the findings based on severity level.

Different levels of severity will be addressed and prioritized within the development ticket tracking system. All vulnerabilities are reviewed and actioned, if required.

Deployment Script Changes and Infrastructure Changes

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

Emergency Changes

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

Availability

Capacity Management

Capacity management is performed on an ongoing basis by all products. The infrastructure and systems that make up each product are continuously monitored for utilization levels and adjusted accordingly.

Backup and Replication

Jira Cloud, Confluence Cloud, JSM and Insight, JPD, Atlas, Atlassian Analytics, and Forge

Atlassian employs Amazon RDS for the above-mentioned products, where each Amazon RDS for each product is unique. Amazon RDS provides high availability and failover support for database (DB) instances using multiple AZ (Multi-AZ) deployments, automatically provisioning and maintaining a synchronous standby replica in a different AZ of the same region to provide data redundancy and failover capability. Multi-AZ is a default setup for Atlassian and is fully managed by AWS including replication issue resolution.

Amazon RDS creates and saves automated backups of the databases. It consists of a snapshot of the Amazon RDS instance, which can be used in conjunction with transaction logs to enable data restore. The backup will be kept for 30 days. On an annual basis, backups are tested for safeguard and recoverability.

Customer data stored in NetApp for Bitbucket Cloud is automatically backed up daily, with data stored in Amazon S3 backed up using versioning functionality. On an annual basis, backups are tested to ensure recoverability.

Bitbucket Cloud

Aurora has been configured for high availability and failover support for DB instances using Multi-AZ deployments. In an AZ failover scenario where the AZ in which the primary node was running went dark, a replica in the working AZ would automatically be promoted to the primary.

Aurora creates and saves automated backups of databases. It consists of a snapshot of the Aurora instance, which can be used in conjunction with transaction logs to enable data restore. The backup will be kept for 30 days and tested annually to ensure recoverability.

Bitbucket Pipelines

All customer data and settings are stored within DDB, managed by the internal PaaS, and protecting tables from accidental write or delete operations through PITR. If these tables become corrupt or truncated, PITR allows recovery of data from any point in time to within 5 minutes, over the last 35 days, to the last known good state.

Compass

DDB and Elasticsearch provide high availability and failover support for DB instances using Multi-AZ deployments, automatically provisioning and maintaining a synchronous standby replica in a different AZ of the same region to provide data redundancy and failover capability. Multi-AZ is a default setup for Atlassian and is fully managed by AWS including replication issue resolution.

All customer data and settings are stored within DDB, managed by the internal PaaS, and protecting tables from accidental write or delete operations through PITR. If these tables become corrupt or truncated, PITR allows recovery of data from any point in time to within 5 minutes, over the last 35 days, to the last known good state.

Elasticsearch automatically generates hourly snapshots that can be restored in the event of data loss. The last 336 snapshots of a cluster are always kept and expire after 14 days. In addition to automated snapshots, the internal PaaS platform takes hourly snapshots that are stored in Amazon S3 buckets. These can be used in the event of an accidental cluster deletion or for replication to a different cluster.

Data Lake

Leveraging the internal PaaS, hourly snapshots are taken, stored in Amazon S3 buckets, and retained for 30 days. These can be used in the event of an accidental cluster deletion or for replication to a different cluster offering backup and restoration capabilities.

Opsgenie

Opsgenie uses AWS fully managed database services (DDB, Amazon S3, and AWS KMS) for storing and processing data. These services span multiple availability zones, with zones running master nodes isolated from each other. AWS provides built-in, high availability, scalability, reliability, and automatic data recovery in the event of data loss.

Opsgenie also relies on AWS partially managed services (ElastiCache Redis, Amazon RDS, and Elasticsearch), with Multi-AZ replication capability. Unlike the serverless approach, Opsgenie is responsible for configuring several zones, instances, and replication, while AWS is responsible for the physical server management. AWS provides automatic failover, but Opsgenie can initiate zone-based failovers as well.

Opsgenie replicates all data changes from Oregon and Frankfurt to their backup AWS regions, Ohio and Ireland respectively, in near real time, meaning the backup region is a copy of the active region. Opsgenie continuously ensures that the backup region is ready for receiving traffic in the event of the active region being fully down or part of a critical service in the active region being down. As such, Opsgenie's infrastructure and backup are replicated on a continuous basis using AWS.

Disaster Recovery

A disaster recovery policy is in place and is reviewed on an annual basis by the disaster recovery steering committee. Procedures for disaster recovery execution are defined, reviewed, tested, and in place. The policy describes, at a high level, the purpose, objectives, scope, critical dependencies, recovery time objective/recovery point objective (RTO/RPO), and roles and responsibilities. Atlassian follows ISO22301 Business Continuity as a guideline for its disaster recovery program.

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

Confidentiality

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

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

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

Complementary User Entity Controls (CUECs)

The Company's controls related to the Atlassian Platform cover only a portion of overall internal control for each user entity of the Atlassian Platform. 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. • 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. • 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 and SSO setup, password settings, and restricting public access). • Customers are responsible for changing their passwords to reflect a minimum length of at least eight characters where they have migrated from another identity service. • Customers are responsible for the safeguarding of their own account access credentials, including passwords or API keys and tokens.
CC6.6 CC6.8 C1.1 C1.2	• Customers are responsible for the 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 CC6.3	• Customers are responsible for managing access rights, including privileged access. • Customers are responsible for requesting, approving, and monitoring Atlassian's customer support access to their account.
CC6.2 CC6.3 C1.2	• Customers are responsible for requesting removal of their account.
CC6.6 CC6.7 CC6.8	• Customers are responsible for ensuring that their machines, devices, and network are secured.
CC7.3	• Customers are responsible for alerting Atlassian of incidents (related to security, availability, and confidentiality) when they become aware of them.
A1.2	• Bitbucket-specific -- Customers are responsible for performing periodic backups of their accounts and repositories for data beyond seven days. • Forge-specific -- Application developers are responsible for maintaining backups of their application code.

Subservice Organization and Complementary Subservice Organization Controls (CSOCs)

The Company uses AWS as a subservice organization for data center colocation services. The Company's controls related to the Atlassian Platform cover only a portion of the overall internal control for each user entity of the Atlassian Platform. 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.

Although the subservice organization has 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 organization. CSOCs are expected to be in place at AWS related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. AWS' physical security controls should mitigate the risk of unauthorized access to the hosting facilities. AWS' environmental protection controls should mitigate the risk of fires, power loss, climate, and temperature variabilities.

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

It is not feasible for the service commitments, system requirements, and applicable criteria related to the Atlassian Platform 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 as described below.

Criteria	Complementary Subservice Organization Controls
CC6.1 CC6.2 CC6.3	• AWS is responsible for IT access above least privileged, including administrator access, and is responsible for approval by appropriate personnel prior to access provisioning. • AWS is responsible for privileged IT access reviews on a regular basis. • AWS is responsible for timely revocation of user access upon termination. • AWS is responsible for encrypting data in transit.
CC6.4	• AWS is 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. • AWS is responsible for approving requests for physical access privileges from an authorized individual.
CC6.5 CC6.7	• AWS is responsible for securely decommissioning and physically destroying production assets in its control.

Criteria	Complementary Subservice Organization Controls
CC7.1 CC7.2 CC7.3	• AWS is responsible for implementing and monitoring electronic intrusion detection systems that can detect breaches into data center server locations. • AWS is responsible for documenting procedures for the identification and escalation of potential security breaches. • AWS is responsible for requiring visitors to be signed in by an authorized workforce member before gaining entry and always escorting them.
CC7.2 A1.2	• AWS is responsible for installing environmental protection that include the following: cooling systems, battery and generator backups, smoke detection, and dry pipe sprinklers. • AWS is responsible for monitoring the environmental protection equipment for incidents or events that impact assets.
CC8.1	• AWS is responsible for ensuring that changes are authorized, tested, and approved prior to implementation.

Specific Criteria Not Relevant to the System

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

Significant Changes to the System

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

Report Use

The description does not omit or distort information relevant to the Atlassian Platform 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 Conduct, Policies and Procedures and Human Resources.

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

Description of Tests Performed by Coalfire Controls, LLC

Our tests of operating effectiveness of controls included such tests as were considered necessary in the circumstances to evaluate whether those controls, and the extent of compliance with them, were sufficient to provide reasonable, but not absolute, assurance that the trust services security, availability, and confidentiality categories and criteria were achieved throughout the period October 1, 2021 to September 30, 2022. In selecting particular tests of the operating effectiveness of the controls, we considered (i) the nature of the controls being tested; (ii) the types of available evidential matter; (iii) the nature of the criteria to be achieved; (iv) the assessed level of control risk; and (v) the expected efficiency and effectiveness of the test. Such tests were used to evaluate fairness of the presentation of the description of the Atlassian Platform 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.		
HR-3	Background checks are performed prior to an employee's start date. Results are reviewed against a results matrix and escalated to Legal and Head of HR Operations, if needed.	Inspected background check completion evidence for a sample of new employees to determine that background checks were performed prior to their start date and that the results were reviewed against a results matrix and escalated to Legal and Head of HR Operations, if needed.	No exceptions noted.
HR-4	Employees and contractors are required to sign CIIAs as part of the onboarding process.	Inspected signed confidentiality agreements for a sample of employees and contractors onboarded during the period to determine that CIIAs were signed prior to start date.	No exceptions noted.
HR-5	Employees and contractors acknowledge the Code of Conduct annually.	Inspected the Code of Conduct to determine that it described employee and contractor responsibilities and expected behavior regarding data and information system usage.	No exceptions noted.
		Inspected acknowledgements for a sample of employees and contractors to determine that employees and contractors acknowledged that they had read and agreed to the Code of Conduct.	No exceptions noted.

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

Control Environment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
ELC-7	An Audit Committee meeting calendar and general meeting agenda are developed.	Inspected the Audit Committee meeting minutes for a sample of quarters to determine that the Audit Committee meeting calendar and general meeting agenda were developed.	No exceptions noted.
ELC-8	At least annually, the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) review committee charters and corporate governance which define their roles, responsibilities, meeting frequency, participants, member qualifications and discussion topics.	Inspected the Board of Directors meeting minutes to determine that the Board of Directors met during the period and its various subcommittees reviewed committee charters and corporate governance that defined roles, responsibilities, meeting frequency, participants, member qualifications and discussion topics.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		
ELC-1	The organizational charts are reviewed by appropriate Atlassian management and updated semi-annually.	Inspected review documentation for a sampled organizational chart review to determine that the organizational charts were reviewed by appropriate Atlassian management and updated semi-annually.	No exceptions noted.
ELC-2	Organizational charts are updated based on employee action notices and available to all Atlassian employees via Workday.	Inspected the organizational charts to determine that they are updated based on employee action notices and available to all Atlassian employees via Workday.	No exceptions noted.
ELC-5	The process of identifying and reviewing Board of Director Candidates is defined In Nominating and Corporate Governance Committee charter.	Inspected the Nominating and Corporate Governance Committee Charter to determine that the process of identifying and reviewing Board of Director Candidates is defined in the Nominating and Corporate Governance Committee charter.	No exceptions noted.

Control Environment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
ELC-14	Management has established defined roles and responsibilities to oversee the implementation of the security and control environment.	Inspected the information security policy to determine that management had established defined roles and responsibilities to oversee the implementation of the security and control environment.	No exceptions noted.
HR-1	The hiring manager reviews and approves job descriptions.	Inspected job descriptions for a sample of employees supporting the service to determine that job descriptions were documented, reviewed and approved by the hiring manager, and included authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
HR-1	The hiring manager reviews and approves job descriptions.	Inspected job descriptions for a sample of employees supporting the service to determine that job descriptions were documented, reviewed and approved by the hiring manager and included authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	No exceptions noted.
HR-2	Job offers to external candidates are approved prior to hiring.	Inspected approval documentation for a sample of new hires to determine that job offers to external candidates are approved prior to hiring.	No exceptions noted.
HR-7	Performance appraisals are performed at least annually.	Inspected performance appraisal documentation for a sample of employees to determine that performance appraisals were completed by management during the period.	No exceptions noted.

Control Environment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
HR-8	Training is available to employees to support their continued development and growth.	Inspected training tools made available to all employees to determine that training is available to employees to support their continued development and growth.	No exceptions noted.
HR-9	User awareness training is performed at least annually for employees and contractors as part of the Atlassian Security Awareness program.	Inspected training completion evidence for a sample of employees and contractors to determine that user awareness training was performed at least annually as part of the Atlassian Security Awareness program.	Exceptions noted. For 3 of 44 employees and contractors sampled, user awareness training was not completed during the period.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
HR-1	The hiring manager reviews and approves job descriptions.	Inspected job descriptions for a sample of employees supporting the service to determine that job descriptions were documented, reviewed and approved by the hiring manager and included authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	No exceptions noted.
HR-5	Employees and contractors acknowledge the Code of Conduct annually.	Inspected the Code of Conduct to determine that it described employee and contractor responsibilities and expected behavior regarding data and information system usage.	No exceptions noted.
		Inspected acknowledgements for a sample of employees and contractors to determine that employees and contractors acknowledged that they had read and agreed to the Code of Conduct.	No exceptions noted.

Control Environment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
HR-7	Performance appraisals are performed at least annually.	Inspected performance appraisal documentation for a sample of employees to determine that performance appraisals were completed by management during the period.	No exceptions noted.
HR-10	The Company has documented disciplinary actions in a formalized sanctions policy for employees and contractors who violate the Code of Conduct.	Inspected the Code of Conduct to determine that the Company had documented disciplinary actions in a formalized sanctions policy for employees and contractors who violated the Code of Conduct.	No exceptions noted.

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

Communication and Information			
TSC Reference	**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.		
CMC-2	A description of the system delineating the boundaries and describing relevant components are documented on the Atlassian intranet and the customer facing website.	Inspected Atlassian's customer facing website and Atlassian intranet to determine that a description of the system delineating the boundaries and describing relevant components are documented on the Atlassian intranet and the customer facing website.	No exceptions noted.
CMC-7	System changes are communicated to internal and external users via a publicly accessible site.	Inspected internal and external release notes page to determine that system changes were communicated to internal and external users via a publicly accessible site.	No exceptions noted.
ELC-10	The Executive team sets strategic operational objectives annually.	Inspected strategy and planning documentation to determine that the Executive team set strategic operational objectives during the period.	No exceptions noted.
ELC-12	Atlassian has established a Whistleblower hotline that is accessible to both external individuals and employees within the Company.	Inspected the Whistleblower hotline communication channels to determine that Atlassian had established a Whistleblower hotline that was accessible to both external individuals and employees within the Company.	No exceptions noted.
ELC-14	Management has established defined roles and responsibilities to oversee the implementation of the security and control environment.	Inspected the information security policy to determine that management had established defined roles and responsibilities to oversee the implementation of the security and control environment.	No exceptions noted.

Communication and Information			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
HR-1	The hiring manager reviews and approves job descriptions.	Inspected job descriptions for a sample of employees supporting the service to determine that job descriptions were documented, reviewed and approved by the hiring manager and included authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	No exceptions noted.
HR-9	User awareness training is performed at least annually for employees and contractors as part of the Atlassian Security Awareness program.	Inspected training completion evidence for a sample of employees and contractors to determine that user awareness training was performed at least annually as part of the Atlassian Security Awareness program.	Exceptions noted. For 3 of 44 employees and contractors sampled, user awareness training was not completed during the period.

Communication and Information			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.		
BBPL-30	**For Bitbucket Cloud:** Bitbucket Cloud uses tools to monitor the availability of customer-facing services. The availability is published so that customers may check the status or uptime of Bitbucket Cloud.	**For Bitbucket Cloud:** Inspected the Bitbucket status page to determine that Bitbucket used tools to monitor the availability of customer-facing services and that the availability was published so that customers could check the status or uptime of Bitbucket Cloud.	No exceptions noted.
CMC-1	Significant changes made to the system are communicated to customers via the Atlassian customer facing website.	Inspected the Atlassian website to determine significant changes to the system are communicated to customers through the customer facing website.	No exceptions noted.
CMC-2	A description of the system delineating the boundaries and describing relevant components are documented on the Atlassian intranet and the customer facing website.	Inspected Atlassian's customer facing website and Atlassian intranet to determine that a description of the system delineating the boundaries and describing relevant components are documented on the Atlassian intranet and the customer facing website.	No exceptions noted.
CMC-3	Terms of Service (ToS) are standardized and approved by Legal. The Atlassian Trust Security page, Privacy Policy, and ToS communicates Atlassian's commitments and the customer responsibilities. The Atlassian Trust Security page, Privacy Policy, and ToS are published on the Atlassian customer facing website and any changes are communicated.	Inspected the Atlassian Trust Security page, Privacy Policy, and ToS to determine that the Company's commitments and the customer responsibilities were communicated to customers.	No exceptions noted.
		Inspected the customer facing website to determine that the Atlassian Trust Security page and ToS were published and any changes to the Atlassian Trust Security page or ToS were communicated.	No exceptions noted.

Communication and Information			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CMC-4	Atlassian communicates changes to confidentiality commitments to its customers, vendors, and internal users through the Atlassian website, when applicable.	Inspected the Atlassian website to determine that Atlassian communicated changes to confidentiality commitments to its customers, vendors, and internal users through the Atlassian website, when applicable.	No exceptions noted.
CMC-6	Users may report bugs, defects, or availability, security, and confidentiality issues.	Inspected the customer reporting portal to determine that an external-facing support system was in place that allowed users to report system information on bugs; defects; or availability, security, and confidentiality issues.	No exceptions noted.
PL-15	Opsgenie publishes availability for the Atlassian Platform so that customers can check status and uptime metrics.	Inspected Opsgenie status page to determine that Opsgenie published availability of the Atlassian Platform so customers could check status and uptime metrics.	No exceptions noted.
VDR-1	Vendor agreements include security, availability, and confidentiality commitments, and are reviewed during the procurement process.	Inspected contracts for a sample of critical vendors to determine that formal information sharing agreements were reviewed during the procurement process and included any applicable security, availability and confidentiality commitments.	No exceptions noted.

Risk Assessment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.		
RM-1	The Atlassian Risk and Compliance team evaluates the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Atlassian maintains a risk and controls matrix within its GRC Tool.	Inspected the Atlassian GRC Tool to determine that the Atlassian Risk and Compliance team evaluated the design of controls and mitigation strategies during the period, including identifying risks and recommending changes in the control environment.	No exceptions noted.
		Inspected the Atlassian GRC Tool to determine that Atlassian maintained a risk and controls matrix within its GRC Tool.	No exceptions noted.
RM-2	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 Atlassian had defined an ERM process.	No exceptions noted.
		Inspected risk assessment documentation to determine that an enterprise risk assessment was conducted during the period and 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.		
DR-1	A disaster recovery policy is in place and is reviewed on an annual basis by the disaster recovery steering committee.	Inspected the disaster recovery policy and review documentation to determine that a disaster recovery policy is in place and is reviewed on an annual basis by the disaster recovery steering committee.	No exceptions noted.

Risk Assessment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
RM-2	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 Atlassian had defined an ERM process.	No exceptions noted.
		Inspected risk assessment documentation to determine that an enterprise risk assessment was conducted during the period and included key product stakeholders.	No exceptions noted.
RM-3	A fraud risk assessment is performed annually by the Head of Risk and Compliance. A cross functional survey of employees in areas susceptible to fraud is conducted and combined with an evaluation of external risks. Results are evaluated by the Head of Risk and Compliance. The results are included with the enterprise risk assessment that is communicated to the board and executive level managers annually.	Inspected fraud risk assessment documentation to determine that a fraud risk assessment was performed by the Head of Risk and Compliance during the period and results were included as a part of the enterprise risk assessment, which was communicated to the board and executive level managers annually.	No exceptions noted.
		Inspected fraud risk assessment documentation to determine that a cross-functional survey of employees in areas susceptible to fraud was conducted and combined with an evaluation of external risks and that results were evaluated by the Head of Risk and Compliance.	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.		
RM-2	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 Atlassian had defined an ERM process.	No exceptions noted.
		Inspected risk assessment documentation to determine that an enterprise risk assessment was conducted during the period and 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**
RM-3	A fraud risk assessment is performed annually by the Head of Risk and Compliance. A cross functional survey of employees in areas susceptible to fraud is conducted and combined with an evaluation of external risks. Results are evaluated by the Head of Risk and Compliance. The results are included with the enterprise risk assessment that is communicated to the board and executive level managers annually.	Inspected fraud risk assessment documentation to determine that a fraud risk assessment was performed by the Head of Risk and Compliance during the period and results were included as a part of the enterprise risk assessment, which was communicated to the board and executive level managers annually.	No exceptions noted.
		Inspected fraud risk assessment documentation to determine that a cross-functional survey of employees in areas susceptible to fraud was conducted and combined with an evaluation of external risks and that results were evaluated by the Head of Risk and Compliance.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.		
MTR-3	Penetration testing is performed by a bug bounty program on a continuous basis. Issues are reviewed, prioritized, and resolved within the defined time frame.	Inspected the penetration test report from the bug bounty program for the period to determine that penetration testing was performed during the period by a bug bounty program on a continuous basis.	No exceptions noted.
		Inspected Jira tickets for a sample of vulnerabilities to determine that vulnerabilities were reviewed, prioritized, and resolved within the defined time frame.	No exceptions noted.

Risk Assessment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
RM-2	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 Atlassian had defined an ERM process.	No exceptions noted.
		Inspected risk assessment documentation to determine that an enterprise risk assessment was conducted during the period and included key product stakeholders.	No exceptions noted.
RM-3	A fraud risk assessment is performed annually by the Head of Risk and Compliance. A cross functional survey of employees in areas susceptible to fraud is conducted and combined with an evaluation of external risks. Results are evaluated by the Head of Risk and Compliance. The results are included with the enterprise risk assessment that is communicated to the board and executive level managers annually.	Inspected fraud risk assessment documentation to determine that a fraud risk assessment was performed by the Head of Risk and Compliance during the period and results were included as a part of the enterprise risk assessment, which was communicated to the board and executive level managers annually.	No exceptions noted.
		Inspected fraud risk assessment documentation to determine that a cross-functional survey of employees in areas susceptible to fraud was conducted and combined with an evaluation of external risks and that results were evaluated by the Head of Risk and Compliance.	No exceptions noted.

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

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

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

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

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

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

Logical and Physical Access Controls			
TSC Reference	**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.		
BBPL-6	**For Bitbucket Cloud and Bitbucket Pipelines:** Customer data is logically isolated.	**For Bitbucket Cloud and Bitbucket Pipelines:** Inspected system configurations to determine that customer data was logically isolated.	No exceptions noted.
BBPL-7	**For Bitbucket Cloud and Bitbucket Pipelines:** Active Bitbucket Cloud customers authenticate via an Atlassian account where password configuration settings are managed.	**For Bitbucket Cloud and Bitbucket Pipelines:** Inspected system configurations to determine that active Bitbucket Cloud customers authenticated via an Atlassian account where password configuration settings were managed.	No exceptions noted.
BBPL-26	**For Bitbucket Cloud and Bitbucket Pipelines:** Bitbucket data is encrypted at rest.	**For Bitbucket Cloud and Bitbucket Pipelines:** Inspected data store configurations to determine that Bitbucket data was encrypted at rest.	No exceptions noted.
DS-3	A ZeroTrust infrastructure is implemented to place endpoints into a tiered network (i.e., High, Trusted, Open) based on their security posture and type of device. Applications added to the SSO platform are tiered according to the ZeroTrust policy. Endpoints cannot access applications via the SSO platform unless they are placed on the same or a higher tier as the application.	Inspected the ZeroTrust Service Tier Standard and the Endpoint Minimum Baseline Configuration Standard and observed applications on the SSO platform to determine that a ZeroTrust infrastructure was implemented to place endpoints into a tiered network (e.g., High, Trusted, Open) based on their security posture and type of device.	No exceptions noted.
		Inspected the ZeroTrust Service Tier Standards and the Endpoint Minimum Baseline Configuration Standard to determine that applications added to the SSO platform were tiered according to the ZeroTrust policy.	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 an endpoint without required configurations and tier placement per the Endpoint Minimum Baseline Configuration Standard to determine that endpoints could not access applications via the SSO platform unless they were placed on the same/higher tier as the application.	No exceptions noted.
IAM-1	Two-factor authentication is required when logging into VPN (Remote Access Service) from any IP address.	Inspected system configurations and observed a remote login session to determine that two-factor authentication was required when logging into VPN (Remote Access Service) from any IP address.	No exceptions noted.
IAM-5	Active Directory (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.
		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.
MICROS-3	**For Bitbucket Cloud, Bitbucket Pipelines, Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Data Lake, Atlassian Analytics, Atlas, Opsgenie, and Compass:** Direct access to the Micros Platform via JumpBox requires a valid SSH key and two-factor authentication.	**For Bitbucket Cloud, Bitbucket Pipelines, Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Data Lake, Atlassian Analytics, Atlas, Opsgenie, and Compass:** Observed a remote login session and inspected system configurations to determine that direct access to the Micros Platform via JumpBox required a valid SSH key and two-factor authentication.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
OG-3	**For Opsgenie:** Opsgenie assigns unique identifiers to customer data upon creation, which is used to segregate customer data.	**For Opsgenie:** Inspected system configurations to determine that Opsgenie assigned unique identifiers to customer data upon creation that was used to segregate customer data.	No exceptions noted.
OG-11	**For Opsgenie:** Encryption is enabled for Opsgenie data at rest.	**For Opsgenie:** Inspected data store configurations to determine that encryption was enabled for Opsgenie data at rest.	No exceptions noted.
PL-3	**For Jira Cloud, JPD, Atlas, Confluence Cloud, JSM and Insight, Forge, Compass, Atlassian Analytics, and Data Lake:** Customer data is logically segregated via unique identifiers that are attached for the lifetime of the data. The unique identifiers are used to determine which users can see which data.	**For Jira Cloud, JPD, Atlas, Confluence Cloud, JSM and Insight, Forge, Compass, Atlassian Analytics, and Data Lake:** Inspected system configurations to determine that customer data was logically segregated via unique identifiers that were attached for the lifetime of the data and that the unique identifiers were used to determine which users could see which data.	No exceptions noted.
PL-4	**For Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Compass, Opsgenie, Atlassian Analytics, and Data Lake:** Unless an external identity provider is implemented by the customer, cloud customers must have a password that is, at a minimum, eight characters in length.	**For Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Compass, Opsgenie, Atlassian Analytics, and Data Lake:** Inspected customer password configurations to determine that, unless an external identity provider was implemented by the customer, cloud customers had to have a password that was, at a minimum, eight characters in length.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
PL-10	**For Jira Cloud, JPD, and Confluence Cloud:** Data that contains attachment contents are encrypted.	**For Jira Cloud, JPD, and Confluence Cloud:** Inspected data store configurations to determine that data that contained attachment contents were encrypted.	No exceptions noted.
PL-11	**For Jira Cloud, JPD, Atlas, Confluence Cloud, JSM and Insight, Compass, Forge, Atlassian Analytics, and Data Lake:** Encryption is enabled for data at rest.	**For Jira Cloud, JPD, Atlas, Confluence Cloud, JSM and Insight, Compass, Forge, Atlassian Analytics, and Data Lake:** Inspected encryption configurations to determine that encryption was enabled for 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.		
BBPL-3	**For Bitbucket Cloud and Bitbucket Pipelines:** Access to a customer repository is supported by a customer support request or internal incident.	**For Bitbucket Cloud and Bitbucket Pipelines:** Inspected system configurations to determine that access to a customer repository was supported by a customer support request or internal incident.	No exceptions noted.
BBPL-5	**For Bitbucket Cloud and Bitbucket Pipelines:** Access to customer repositories by the Bitbucket internal support team is reviewed quarterly by the lead Support Engineer.	**For Bitbucket Cloud and Bitbucket Pipelines:** Inspected access review documentation for a sample of quarters to determine that access to customer repositories by the Bitbucket internal support team was reviewed quarterly by the lead Support Engineer.	Exception noted. Atlassian Internal Audit identified that the quarterly access reviews did not include all user groups with access to Bitbucket and Bitbucket Pipelines customer repositories.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
BBPL-13	**For Bitbucket Cloud:** Privileged access to the software that the Bitbucket Cloud team uses to administer the service is reviewed semi-annually.	**For Bitbucket Cloud:** Inspected access review documentation for a sample semi-annual reviews to determine that privileged access to the software that the Bitbucket Cloud team used to administer the service was reviewed semi-annually.	No exceptions noted.
DTL-1	Access to customer data is restricted to administrators and is only granted to developers on an as-needed and temporary basis to troubleshoot incidents.	Inspected code configurations to determine that access to customer data was restricted to administrators and was only granted to developers on an as-needed and temporary basis to troubleshoot incidents.	No exceptions noted.
		Inspected access tickets for a sample of developers granted access to customer data to determine that access was only granted to developers on an as-needed and temporary basis to troubleshoot incidents.	No exceptions noted.
IAM-3	Access to the Atlassian internal network and internal tools is restricted to authorized users via the following logical access measures: - Each Atlassian user must have an active Active Directory (AD) account - Each Atlassian user must be a member of the appropriate LDAP group	Inspected system configurations and observed logins to the Atlassian internal network and tools to determine that access to the Atlassian internal network and internal tools was restricted to authorized users via the following logical access measures: - Each Atlassian user must have an active AD account - Each Atlassian user must be a member of the appropriate LDAP 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**
IAM-4	AD group membership is automatically assigned based on the user's department and team.	Inspected system configurations to determine that AD group membership was automatically assigned based on the user's department and team.	No exceptions noted.
IAM-6	An automatic alert is triggered to the WPT or HR Information Systems Manager for any role change between the following groups: Engineering, Customer Support & Success (CSS), or Finance. Appropriateness of access is reviewed and approved.	Inspected alert threshold configurations and an example alert to determine that automatic alerts were triggered to the WPT or HR Information Systems Manager for any role change between the following groups: Engineering, CSS, or Finance.	No exceptions noted.
		Inspected access review and approval documentation for a sample of alerts to determine that appropriateness of access was reviewed and approved.	No exceptions noted.
IAM-7	AD accounts and network access are automatically disabled within eight 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 was set to be automatically disabled within eight hours from the time an employee was marked as terminated in the HR system.	No exceptions noted.
IAM-8	The HR system does not allow terminations to be backdated.	Observed a demonstration of the HR system to determine that the HR system did not allow terminations to be backdated.	No exceptions noted.
IAM-9	Semi-annually, the Build Engineering Development Team Lead performs a review of privileged user access for Deployment Bamboo.	Inspected user access review documentation for a sample of semi-annual reviews to determine that the Build Engineering Development Team Lead performed a review of privileged user access for Deployment Bamboo semi-annually.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
IAM-11	The People Central Systems Support Specialist performs a review over Workday admin users semi-annually.	Inspected user access review documentation for a sample of semi-annual reviews to determine that the People Central Systems Support Specialist performed a review over Workday admin users semi-annually.	No exceptions noted.
IAM-12	**For Bitbucket Cloud, Bitbucket Pipelines, Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Data Lake, Atlassian Analytics, and Compass:** Access to critical systems and services that the Bitbucket Pipelines team uses to administer the service is reviewed semi-annually.	**For Bitbucket Cloud, Bitbucket Pipelines, Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Data Lake, Atlassian Analytics, and Compass:** Inspected user access review documentation for a sample of semi-annual reviews to determine that access to critical systems and services that the Bitbucket Pipelines team used to administer the service were reviewed semi-annually.	No exceptions noted.
IAM-14	**For Bitbucket Cloud, Bitbucket Pipelines, Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Data Lake, Atlassian Analytics, and Compass:** The Build Engineering team performs a semi-annual access review for Artifactory.	**For Bitbucket Cloud, Bitbucket Pipelines, Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Data Lake, Atlassian Analytics, and Compass:** Inspected user access review documentation for a sample of semi-annual reviews to determine that the Build Engineering team performed an access review for Artifactory semi-annually.	No exceptions noted.
IAM-16	Administrative access to SSAM is provisioned based on appropriate authorization by the service owner or delegate.	Inspected the access listings, inquired of management, and compared each user's level of access to their job role to determine that administrative access to SSAM was provisioned based on appropriate authorization by the service owner or delegate.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
IAM-17	User access reviews for Kubernetes and SSAM containers are performed semi-annually, and issues identified are remediated in a timely manner.	Inspected user access review documentation for a sample of semi-annual reviews to determine that user access reviews for Kubernetes and SSAM containers were performed semi-annually and issues identified were remediated in a timely manner.	No exceptions noted.
MICROS-5	**For Bitbucket Cloud, Bitbucket Pipelines, Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Data Lake, Atlassian Analytics, Atlas, and Compass:** Access to the AWS production environment, RDS databases, and supporting tools is provisioned based on appropriate authorization by the service owner or delegate.	**For Bitbucket Cloud, Bitbucket Pipelines, Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Data Lake, Atlassian Analytics, Atlas, and Compass:** Inspected the access log to determine that access to the AWS production environment, RDS databases, and supporting tools was provisioned based on appropriate authorization by the service owner or delegate.	No exceptions noted.
MICROS-6	**For Bitbucket Cloud, Bitbucket Pipelines, Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Data Lake, Atlassian Analytics, and Compass:** Atlassian's Engineering Managers or Team Leads perform a user access review over the Micros Platform and the associated in-scope supporting databases, tools, and services semi-annually.	**For Bitbucket Cloud, Bitbucket Pipelines, Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Data Lake, Atlassian Analytics, and Compass:** Inspected access review documentation for a sample of semi-annual reviews to determine that Atlassian's Engineering Managers or Team Leads performed a user access review over the Micros Platform and the associated in-scope supporting databases, tools, and services semi-annually.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
OG-2	**For Opsgenie:** Access to customer data by the Opsgenie Support team is supported by a valid and approved customer support request.	**For Opsgenie:** Inspected system configurations to determine that access to customer data by the Opsgenie Support team is supported by a valid and approved customer support request.	Exception noted. Atlassian Internal Audit identified that an Opsgenie support member was able to continue accessing customer data without a valid customer support request.
OG-6	**For Opsgenie:** The Opsgenie user access review is performed semi-annually, and a review of shared, generic, and bot accounts is performed annually. Tickets are created to remove or modify access as necessary in a timely manner.	**For Opsgenie:** Inspected user access review documentation for a sample semi-annual reviews to determine that an Opsgenie user access review was performed semi-annually and that tickets were created to remove or modify access as necessary in a timely manner.	No exceptions noted.
		For Opsgenie: Inspected access review documentation to determine that a review of shared, generic, and bot accounts was performed during the period and that tickets were created to remove or modify access as necessary in a timely manner.	No exceptions noted.
OG-8	**For Opsgenie:** Access is approved prior to provisioning access.	**For Opsgenie:** Inspected the Opsgenie access provisioning logs to determine that access to Opsgenie systems was formally requested and approved prior to 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**
PL-2	**For Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Data Lake, Atlassian Analytics, Atlas, Forge, and Compass:** Customer data is only accessed when supported by a valid customer support request or an active incident that requires access.	**For Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Data Lake, Atlassian Analytics, Atlas, Forge, and Compass:** Inspected evidence of code configurations to determine that customer data could only be accessed when supported by a valid customer support request or an active incident that required access.	No exceptions noted.
PL-6	**For Forge, Data Lake, Atlassian Analytics, Atlas, and JSM and Insight:** User access reviews are performed semi-annually, and issues identified are remediated in a timely manner.	**For Forge, Data Lake, Atlassian Analytics, Atlas, and JSM and Insight:** Inspected user access review documentation for a sample semi-annual reviews to determine that user access reviews were performed semi-annually and issues identified were remediated in a timely manner.	Exceptions noted. Atlassian Internal Audit identified that a user access review for Data Lake did not occur during the period.
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.		
BBPL-3	**For Bitbucket Cloud and Bitbucket Pipelines:** Access to a customer repository is supported by a customer support request or internal incident.	**For Bitbucket Cloud and Bitbucket Pipelines:** Inspected system configurations to determine that access to a customer repository was supported by a customer support request or internal incident.	No exceptions noted.
BBPL-4	**For Bitbucket Cloud and Bitbucket Pipelines:** Access to the Bitbucket Cloud Django Admin group is restricted to appropriate Atlassian team members.	**For Bitbucket Cloud and Bitbucket Pipelines:** Inspected the Bitbucket Cloud Django Admin group provisioning logs to determine that access was restricted to appropriate Atlassian team members.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
DTL-1	Access to customer data is restricted to administrators and is only granted to developers on an as-needed and temporary basis to troubleshoot incidents.	Inspected code configurations to determine that access to customer data was restricted to administrators and was only granted to developers on an as-needed and temporary basis to troubleshoot incidents.	No exceptions noted.
		Inspected access tickets for a sample of developers granted access to customer data to determine that access was only granted to developers on an as-needed and temporary basis to troubleshoot incidents.	No exceptions noted.
IAM-7	AD accounts and network access are automatically disabled within eight 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 was set to be automatically disabled within eight hours from the time an employee was marked as terminated in the HR system.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
IAM-10	On a semi-annual basis, the Active Directory and Idaptive system owner performs a user access review of privileged Active Directory and Idaptive access (including generic accounts) and Active Directory Admin Accounts and any necessary changes are made as a result of the review.	Inspected access review documentation for a sampled access review to determine that the Active Directory and Idaptive system owner performed a user access review of privileged Active Directory and Idaptive access (including generic accounts) and Active Directory Admin Accounts semi-annually.	No exceptions noted.
	A portion of the control did operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No changes were identified as part of the semi-annual Active Directory and Idaptive privileged access reviews.	Inspected change tickets for a sample of changes that resulted from the privileged access review to determine that change tickets were created to track access removals or modifications resulting from the review.	Not tested. No changes were identified as part of the semi-annual Active Directory and Idaptive privileged access reviews.
IAM-13	**For Bitbucket Cloud, Bitbucket Pipelines, Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Data Lake, Atlassian Analytics, and Compass:** Privileged access to Deployment Bamboo is restricted to the members of the Build Engineering team.	**Bitbucket Cloud, Bitbucket Pipelines, Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Data Lake, Atlassian Analytics, and Compass:** Inspected privileged access listings, inquired of management, and compared each user's level of access to their job role to determine that privileged access to Deployment Bamboo was restricted to the members of the Build Engineering team.	No exceptions noted.
IAM-18	Only service owners have the ability to grant and remove delegate access in SSAM.	Inspected system configurations to determine that only service owners had the ability to grant and remove delegate access in SSAM.	No exceptions noted.
IAM-19	Only authorized service owners and delegates have the access to add, modify, and remove access in SSAM containers.	Inspected system configurations to determine that only authorized service owners and delegates had the access to add, modify, and remove access in SSAM containers.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
MICROS-4	**For Bitbucket Cloud, Bitbucket Pipelines, Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Data Lake, Atlassian Analytics, Atlas, and Compass:** Privileged access of Atlassian users to the EC2 production environment is restricted to authorized and appropriate users only.	**For Bitbucket Cloud, Bitbucket Pipelines, Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Data Lake, Atlassian Analytics, Atlas, and Compass:** Inspected privileged access listings, inquired of management, and compared each user's level of access to their job role to determine that privileged access of Atlassian users to the EC2 production environment was restricted to authorized and appropriate users only.	No exceptions noted.
OG-2	**For Opsgenie:** Access to customer data by the Opsgenie Support team is supported by a valid and approved customer support request.	**For Opsgenie:** Inspected system configurations to determine that access to customer data by the Opsgenie Support team is supported by a valid and approved customer support request.	Exception noted. Atlassian Internal Audit identified that an Opsgenie support member was able to continue accessing customer data without a valid customer support request.
OG-5	**For Opsgenie:** No users have access to directly release a build or modify any build artifacts into S3 or deploy a change directly into the Opsgenie production environment.	**For Opsgenie:** Inspected system configurations to determine that no users had access to directly release a build or modify any build artifacts into S3 or deploy a change directly into the Opsgenie production environment.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
OG-7	**For Opsgenie:** Privileged access to AWS services within the AWS console is restricted to authorized and appropriate users.	**For Opsgenie:** Inspected the access listings, inquired of management, and compared each user's level of access to their job role to determine that privileged access to AWS services within the AWS console was restricted to authorized and appropriate users.	No exceptions noted.
PL-2	**For Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Data Lake, Atlassian Analytics, Atlas, Forge, and Compass:** Customer data is only accessed when supported by a valid customer support request or an active incident that requires access.	**For Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Data Lake, Atlassian Analytics, Atlas, Forge, and Compass:** Inspected evidence of code configurations to determine that customer data could only be accessed when supported by a valid customer support request or an active incident that required access.	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 environments are hosted at third-party data centers, which are carved out for the purposes of this report.	Not applicable.	Not applicable.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.		
INV-1	A formal inventory of production system assets that includes asset owners is maintained, and changes to the inventory are logged.	Inspected the production system asset inventory to determine that a formal inventory of production system assets that included asset owners was maintained and changes to the inventory were logged.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
BBPL-27	**For Bitbucket Cloud and Bitbucket Pipelines:** Firewall rules are in place to restrict access to the Bitbucket Cloud production environment.	**For Bitbucket Cloud and Bitbucket Pipelines:** Inspected firewall configurations to determine that firewalls were in place to restrict access to the Bitbucket Cloud production environment.	No exceptions noted.
IAM-1	Two-factor authentication is required when logging into VPN (Remote Access Service) from any IP address.	Inspected system configurations and observed a remote login session to determine that two-factor authentication was required when logging into VPN (Remote Access Service) from any IP address.	No exceptions noted.
IAM-2	Two-factor authentication is required when launching an application from the single sign on system (Idaptive).	Inspected system configurations and observed a remote login session to determine that two-factor authentication was required when launching an application from the single sign on system (Idaptive).	No exceptions noted.
IAM-15	**For JSM and Insight, and Bitbucket Pipelines:** Direct access to Kubernetes environments requires a valid key and two-factor authentication.	**For JSM and Insight, and Bitbucket Pipelines:** Inspected system configurations and observed a remote login session to determine that direct access to Kubernetes environments required a valid key and two-factor authentication.	No exceptions noted.
MICROS-3	**For Bitbucket Cloud, Bitbucket Pipelines, Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Data Lake, Atlassian Analytics, Atlas, Opsgenie, and Compass:** Direct access to the Micros Platform via JumpBox requires a valid SSH key and two-factor authentication.	**For Bitbucket Cloud, Bitbucket Pipelines, Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Data Lake, Atlassian Analytics, Atlas, Opsgenie, and Compass:** Observed a remote login session and inspected system configurations to determine that direct access to the Micros Platform via JumpBox required a valid SSH key and two-factor authentication.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
MTR-4	IT asset management software is used to enforce hard drive encryption, user authentication requirements, and security patching on MacOS endpoints.	Inspected the IT asset management software configurations to determine that IT asset management software was used to enforce hard drive encryption, user authentication requirements, and security patching on MacOS endpoints.	No exceptions noted.
MTR-5	IT asset management software is used to monitor hard drive encryption, user authentication requirements, and security patching on Windows endpoints.	Inspected the IT asset management software configurations to determine that IT asset management software was used to monitor hard drive encryption, user authentication requirements, and security patching on Windows endpoints.	No exceptions noted.
OG-12	**For Opsgenie:** Firewall rules are in place to restrict access to the Opsgenie production environment.	**For Opsgenie:** Inspected firewall configurations to determine that firewalls were in place to restrict access to the production environment.	No exceptions noted.
PL-13	**For Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Compass, Forge, Atlassian Analytics, Atlas, and Data Lake:** Firewall rules are in place; are configured using security policy rules to limit unnecessary ports, protocols, and services; and are maintained by the Micros team. All changes to firewall rules require a peer-reviewed pull request.	**For Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Compass, Forge, Atlassian Analytics, Atlas, and Data Lake:** Inspected firewall configurations to determine that firewalls were in place; were configured using security policy rules to limit unnecessary ports, protocols, and services; and were maintained by the Micros team.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		For Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Compass, Forge, Atlassian Analytics, Atlas, and Data Lake: Inspected a sample of Jira tickets to determine that changes to firewall rules required a peer-reviewed pull request.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.		
BBPL-25	**For Bitbucket Cloud and Bitbucket Pipelines:** External users connect to Bitbucket using encrypted traffic via SSH and TLS certificates. Certificates are rotated and reviewed prior to expiration.	**For Bitbucket Cloud and Bitbucket Pipelines:** Inspected transmission protocol configurations to determine that external users connected to Bitbucket using encrypted traffic via SSH and TLS certificates.	No exceptions noted.
		For Bitbucket Cloud and Bitbucket Pipelines: Inspected certificate expiry notifications and updated certificate expiration dates to determine that certificates were rotated and reviewed prior to expiration.	No exceptions noted.
MTR-4	IT asset management software is used to enforce hard drive encryption, user authentication requirements, and security patching on MacOS endpoints.	Inspected the IT asset management software configurations to determine that IT asset management software was used to enforce hard drive encryption, user authentication requirements, and security patching on MacOS endpoints.	No exceptions noted.
MTR-5	IT asset management software is used to monitor hard drive encryption, user authentication requirements, and security patching on Windows endpoints.	Inspected the IT asset management software configurations to determine that IT asset management software was used to monitor hard drive encryption, user authentication requirements, and security patching on Windows endpoints.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
MTR-7	A mobile device management (MDM) system is in place to centrally manage mobile devices supporting the service.	Inspected the MDM system configurations to determine that an MDM system was in place to centrally manage mobile devices supporting the service.	No exceptions noted.
OG-10	**For Opsgenie:** External users securely connect to Opsgenie via the encrypted TLS protocol.	**For Opsgenie:** Inspected transmission protocol configurations to determine that external users securely connected to Opsgenie via the encrypted TLS protocol.	No exceptions noted.
PL-12	**For Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Compass, Forge, Atlassian Analytics, Atlas, and Data Lake:** External users connect to the Systems using encrypted traffic via TLS protocol. Certificates are rotated upon expiration.	**For Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Compass, Forge, Atlassian Analytics, Atlas, and Data Lake:** Inspected transmission protocol configurations to determine that external users connected to the Systems using encrypted traffic via TLS protocol.	No exceptions noted.
		For Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Compass, Forge, Atlassian Analytics, Atlas, and Data Lake: Inspected certificate expiry notifications and updated certificate expiration dates to determine that certificates were rotated prior to expiration.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.		
MTR-1	Atlassian uses malware protection for Windows and OSX clients. An enterprise anti-malware platform provides endpoint protection, centralized reporting, and notifications. The anti-malware client is installed via management platforms and protected by a complex password to prevent staff from removing or uninstalling the agent.	Inspected anti-malware software configurations to determine that Atlassian used malware protection for Windows and OSX clients that provides endpoint protection, centralized reporting, and notifications.	No exceptions noted.
		Inspected the anti malware software configurations to determine that the anti-malware client was installed via management platforms and was protected by a complex password to prevent staff from removing or uninstalling the agent.	No exceptions noted.
MTR-4	IT asset management software is used to enforce hard drive encryption, user authentication requirements, and security patching on MacOS endpoints.	Inspected the IT asset management software configurations to determine that IT asset management software was used to enforce hard drive encryption, user authentication requirements, and security patching on MacOS endpoints.	No exceptions noted.
MTR-5	IT asset management software is used to monitor hard drive encryption, user authentication requirements, and security patching on Windows endpoints.	Inspected the IT asset management software configurations to determine that IT asset management software was used to monitor hard drive encryption, user authentication requirements, and security patching on Windows endpoints.	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.		
MTR-2	Continuous internal and external vulnerability scanning is performed over the Atlassian environment. Vulnerabilities are reviewed, prioritized, and resolved as per the defined time frame. Vulnerabilities are reviewed, prioritized, and resolved as per the defined time frame.	Inspected continuous internal and external network vulnerability scan configurations to determine that internal and external network vulnerability scans were performed continuously to identify, quantify, and prioritize vulnerabilities.	No exceptions noted.
		Inspected remediation documentation for a sample of vulnerabilities identified during the period to determine that vulnerabilities were resolved within Atlassian's standard resolution time frames.	No exceptions noted.
MTR-4	IT asset management software is used to enforce hard drive encryption, user authentication requirements, and security patching on MacOS endpoints.	Inspected the IT asset management software configurations to determine that IT asset management software was used to enforce hard drive encryption, user authentication requirements, and security patching on MacOS endpoints.	No exceptions noted.
MTR-5	IT asset management software is used to monitor hard drive encryption, user authentication requirements, and security patching on Windows endpoints.	Inspected the IT asset management software configurations to determine that IT asset management software was used to monitor hard drive encryption, user authentication requirements, and security patching on Windows endpoints.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
RM-2	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 Atlassian had defined an ERM process.	No exceptions noted.
		Inspected risk assessment documentation to determine that an enterprise risk assessment was conducted during the period and included key product stakeholders.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.		
BBPL-29	**For Bitbucket Cloud:** Monitoring tools are in place to track and notify on the availability and reliability of Bitbucket Cloud systems and services.	**For Bitbucket Cloud:** Inspected the availability and reliability monitoring tools dashboard and alert configurations to determine that monitoring tools were in place to track and notify on the availability and reliability of Bitbucket Cloud systems and services.	No exceptions noted.
BBPL-31	**For Bitbucket Pipelines:** Monitoring tools are in place to track and notify on the availability and reliability of Bitbucket Pipelines services.	**For Bitbucket Pipelines:** Inspected the availability and reliability monitoring tools dashboard and alert configurations to determine that monitoring tools were in place to track and notify on the availability and reliability of Bitbucket Pipelines services.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
MTR-2	Continuous internal and external vulnerability scanning is performed over the Atlassian environment. Vulnerabilities are reviewed, prioritized, and resolved as per the defined time frame. Vulnerabilities are reviewed, prioritized, and resolved as per the defined time frame.	Inspected continuous internal and external network vulnerability scan configurations to determine that internal and external network vulnerability scans were performed continuously to identify, quantify, and prioritize vulnerabilities.	No exceptions noted.
		Inspected remediation documentation for a sample of vulnerabilities identified during the period to determine that vulnerabilities were resolved within Atlassian's standard resolution time frames.	No exceptions noted.
MTR-3	Penetration testing is performed by a bug bounty program on a continuous basis. Issues are reviewed, prioritized, and resolved within the defined time frame.	Inspected the penetration test report from the bug bounty program for the period to determine that penetration testing was performed during the period by a bug bounty program on a continuous basis.	No exceptions noted.
		Inspected Jira tickets for a sample of vulnerabilities to determine that vulnerabilities were reviewed, prioritized, and resolved within the defined time frame.	No exceptions noted.
MTR-6	A log management tool is utilized to identify trends that may have a potential impact on the Company's ability to achieve its security objectives and generates alerts when specific events occur.	Inspected the log management tool configurations to determine that a log management tool was utilized to identify trends that may have had a potential impact on the Company's ability to achieve its security objectives and generated alerts when specific events occurred.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
OG-13	**For Opsgenie:** Infrastructure and core service status are monitored continuously by AWS CloudWatch. If availability and processing capacity issues are detected in Opsgenie, alerts are sent to the on-call engineers.	**For Opsgenie:** Inspected system configurations to determine that infrastructure and core service status were monitored continuously by AWS CloudWatch.	No exceptions noted.
		For Opsgenie: Inspected alert configurations to determine that, if availability and processing capacity issues were detected in Opsgenie, alerts were sent to the on-call engineers.	No exceptions noted.
PL-14	**For Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Compass, Forge, Atlassian Analytics, Atlas, and Data Lake:** 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. Changes to availability are published online so that customers may check the status of the service.	**For Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Compass, Forge, Atlassian Analytics, Atlas, and Data Lake:** 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.
		For Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Compass, Forge, Atlassian Analytics, Atlas, and Data Lake: Inspected the Atlassian status page to determine that changes to availability were published online so that customers could check the status of the service.	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.		
IM-1	An organizational wide incident management process is in place, with the SRE team responsible for incidents and problems for Atlassian services and platforms. Incident management processes must meet the Atlassian Incident Management Standard.	Inspected the Atlassian Incident Management Standard to determine an organization-wide process was in place and established the SRE team as responsible for incidents and problems for the Atlassian services and platforms.	No exceptions noted.
		Inspected a sample of security events to determine that security events and incidents were addressed in accordance with the Atlassian Incident Management Standard.	No exceptions noted.
MTR-2	Continuous internal and external vulnerability scanning is performed over the Atlassian environment. Vulnerabilities are reviewed, prioritized, and resolved as per the defined time frame. Vulnerabilities are reviewed, prioritized, and resolved as per the defined time frame.	Inspected continuous internal and external network vulnerability scan configurations to determine that internal and external network vulnerability scans were performed continuously to identify, quantify, and prioritize vulnerabilities.	No exceptions noted.
		Inspected remediation documentation for a sample of vulnerabilities identified during the period to determine that vulnerabilities were resolved within Atlassian's standard resolution time frames.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
MTR-3	Penetration testing is performed by a bug bounty program on a continuous basis. Issues are reviewed, prioritized, and resolved within the defined time frame.	Inspected the penetration test report from the bug bounty program for the period to determine that penetration testing was performed during the period by a bug bounty program on a continuous basis.	No exceptions noted.
		Inspected Jira tickets for a sample of vulnerabilities to determine that vulnerabilities were reviewed, prioritized, and resolved within the defined time frame.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.		
IM-1	An organizational wide incident management process is in place, with the SRE team responsible for incidents and problems for Atlassian services and platforms. Incident management processes must meet the Atlassian Incident Management Standard.	Inspected the Atlassian Incident Management Standard to determine an organization-wide process was in place and established the SRE team as responsible for incidents and problems for the Atlassian services and platforms.	No exceptions noted.
		Inspected a sample of security events to determine that security events and incidents were addressed in accordance with the Atlassian Incident Management Standard.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.		
DR-1	A disaster recovery policy is in place and is reviewed on an annual basis by the disaster recovery steering committee.	Inspected the disaster recovery policy and review documentation to determine that a disaster recovery policy is in place and was reviewed during the period by the disaster recovery steering committee.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
IM-1	An organizational wide incident management process is in place, with the SRE team responsible for incidents and problems for Atlassian services and platforms. Incident management processes must meet the Atlassian Incident Management Standard.	Inspected the Atlassian Incident Management Standard to determine an organization-wide process was in place and established the SRE team as responsible for incidents and problems for the Atlassian services and platforms.	No exceptions noted.
		Inspected a sample of security events to determine that security events and incidents were addressed in accordance with the Atlassian Incident Management Standard.	No exceptions noted.
MTR-6	The incident response plan is tested at least annually to assess the effectiveness of the incident response program.	Inspected the incident response plan test results to determine that the incident response plan was tested during the period to assess the effectiveness of the incident response program.	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.		
BBPL-8	**For Bitbucket Cloud:** Merging code to the production branch of Bitbucket Cloud requires a peer-reviewed pull request.	**For Bitbucket Cloud:** Inspected system configurations to determine that merging code to the production branch of Bitbucket Cloud required a peer-reviewed pull request.	No exceptions noted.
CHG-1	Peer review and passed green build testing is required prior to production deployment.	Inspected system configurations to determine that peer review and passed green build testing was required prior to production deployment.	No exceptions noted.
CHG-2	Bitbucket does not allow a pull request to be approved by the same user who requests it.	Inspected system configurations to determine that Bitbucket did not allow a pull request to be approved by the same user who requested it.	No exceptions noted.
CHG-3	**For Bitbucket Cloud, Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Data Lake, Atlassian Analytics, and Compass:** Deployment Bamboo does not allow code to be deployed unless it has passed green build testing.	**For Bitbucket Cloud, Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Data Lake, Atlassian Analytics, and Compass:** Inspected system configurations to determine that Deployment Bamboo would not allow code to be deployed unless it had passed green build testing.	No exceptions noted.

Change Management			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CHG-4	**For Bitbucket Cloud, Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Data Lake, Atlassian Analytics, and Compass:** Deployment Bamboo performs a check to validate that the SOX settings on Bitbucket are compliant with the following: - Requires more than one approver - Unapproved automatically on new changes - Deny changes without a pull request If the settings are not compliant, the code is rejected.	**For Bitbucket Cloud, Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Data Lake, Atlassian Analytics, and Compass:** Inspected system configurations to determine that deployment Bamboo performed a check to validate that the SOX settings on Bitbucket required more than one approver, were unapproved automatically for new changes, and denied changes without a pull request.	No exceptions noted.
		For Bitbucket Cloud, Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Data Lake, Atlassian Analytics, and Compass: Inspected system configurations to determine that deployment Bamboo rejected the code if noncompliant settings were identified.	No exceptions noted.
CHG-5	A Jira ticket is automatically generated if a change to the enforcement of peer review occurs.	Inspected system configurations to determine that a Jira ticket was automatically generated if a change to the enforcement of peer review occurred.	No exceptions noted.
CHG-6	**For Bitbucket Cloud, Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Data Lake, Atlassian Analytics, Atlas, and Compass:** Tokenator performs a check when building code designed for deployment to the SOX namespace on Micros to validate that the Bitbucket Cloud "Compliance" setting is enforced on the branch that the build is occurring from.	**For Bitbucket Cloud, Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Data Lake, Atlassian Analytics, Atlas, and Compass:** Inspected system configurations to determine that Tokenator performed a check when building code designed for deployment to the SOX namespace on Micros to validate that the Bitbucket Cloud "Compliance" setting was enforced on the branch that the build was occurring from.	No exceptions noted.

Change Management			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CHG-7	**For Bitbucket Cloud, Bitbucket Pipelines, Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Data Lake, Atlassian Analytics, Opsgenie, and Compass:** All changes to the master branch of Deployment Bamboo in-scope repositories require a peer-reviewed pull request.	**For Bitbucket Cloud, Bitbucket Pipelines, Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Data Lake, Atlassian Analytics, Opsgenie, and Compass:** Inspected system configurations to determine that all changes to the master branch of Deployment Bamboo in-scope repositories required a peer-reviewed pull request.	No exceptions noted.
CHG-8	**For Bitbucket Cloud, Bitbucket Pipelines, Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Data Lake, Atlassian Analytics, Opsgenie, and Compass:** Changes to the Deployment Bamboo product are tested by the Build Engineering team prior to upgrading internal Deployment Bamboo servers.	**For Bitbucket Cloud, Bitbucket Pipelines, Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Data Lake, Atlassian Analytics, Opsgenie, and Compass:** Inspected system settings to determine that changes to the Deployment Bamboo product were required to be tested by the Build Engineering team prior to upgrading internal Deployment Bamboo servers.	No exceptions noted.
CHG-9	**For Bitbucket Cloud, Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Data Lake, Atlassian Analytics, and Compass:** Changes to Bitbucket Pipelines must be peer reviewed prior to production deployment.	**For Bitbucket Cloud, Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Data Lake, Atlassian Analytics, and Compass:** Inspected the system configurations to determine that changes to Bitbucket Pipelines had to be peer reviewed prior to production deployment.	No exceptions noted.
CHG-10	**For Bitbucket Cloud, Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Data Lake, Atlassian Analytics, Atlas, and Compass:** Bitbucket Pipelines do not allow code to be deployed unless it has passed green build testing.	**For Bitbucket Cloud, Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Data Lake, Atlassian Analytics, Atlas, and Compass:** Inspected the system configurations to determine that Bitbucket Pipelines did not allow code to be deployed unless it had passed green build testing.	No exceptions noted.

Change Management			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CHG-11	**For Bitbucket Cloud, Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Data Lake, Atlassian Analytics, Atlas, and Compass:** Write access to production software artifacts in Artifactory is limited to the Build Engineering team, the automated build system, and the Micros server.	**For Bitbucket Cloud, Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Data Lake, Atlassian Analytics, Atlas, and Compass:** Inspected access listings, access review documentation, and compared each users level of access to their job role to determine that write access to production software artifacts in Artifactory was limited to the Build Engineering team, the automated build system, and the Micros server.	No exceptions noted.
MICROS-1	**For Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Compass, Atlassian Analytics, and Data Lake:** The Micros platform does not allow code artifacts to deploy or run on the platform unless they are peer reviewed and pass green build testing.	**For Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Compass, Atlassian Analytics, and Data Lake:** Inspected system configurations to determine that the Micros platform would not allow code artifacts to be deployed or ran on the platform unless they had been peer reviewed and had passed green build testing.	No exceptions noted.
MICROS-2	Micros only pulls deployment artifacts from the restricted namespace. Only Deployment Bamboo has the credentials to push to the restricted namespace.	Inspected system configurations to determine that Micros only pulled deployment artifacts from the restricted namespace.	No exceptions noted.
		Inspected system configurations to determine that only Deployment Bamboo had the credentials to push to the restricted namespace.	No exceptions noted.

Change Management			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
MTR-8	Code scanning is performed continuously. Vulnerabilities are reviewed continuously and resolved within Atlassian's standard resolution time frames.	Inspected scanning configurations to determine that code scanning was performed continuously.	No exceptions noted
		Inspected Jira tickets to determine that vulnerabilities were reviewed continuously and resolved within Atlassian's standard resolution time frames.	No exceptions noted
OG-4	**For Opsgenie:** Only artifacts that have a valid signature from the build software can be released to the production environment.	**For Opsgenie:** Inspected system configurations to determine that only artifacts that had a valid signature from the build software could be released to the production environment.	No exceptions noted.
OG-5	**For Opsgenie:** No users have access to directly release a build or modify any build artifacts into S3 or deploy a change directly into the Opsgenie production environment.	**For Opsgenie:** Inspected system configurations to determine that no users had access to directly release a build or modify any build artifacts into S3 or deploy a change directly into the Opsgenie production environment.	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.		
DR-1	A disaster recovery policy is in place and is reviewed on an annual basis by the disaster recovery steering committee.	Inspected the disaster recovery policy and review documentation to determine that a disaster recovery policy is in place and is reviewed on an annual basis by the disaster recovery steering committee.	No exceptions noted.
IM-1	An organizational wide incident management process is in place, with the SRE team responsible for incidents and problems for Atlassian services and platforms. Incident management processes must meet the Atlassian Incident Management Standard.	Inspected the Atlassian Incident Management Standard to determine an organization-wide process was in place and established the SRE team as responsible for incidents and problems for the Atlassian services and platforms.	No exceptions noted.
		Inspected a sample of security events to determine that security events and incidents were addressed in accordance with the Atlassian Incident Management Standard.	No exceptions noted.
MTR-6	The incident response plan is tested at least annually to assess the effectiveness of the incident response program.	Inspected the incident response plan test results to determine that the incident response plan was tested during the period to assess the effectiveness of the incident response program.	No exceptions noted.
RM-1	The Atlassian Risk and Compliance team evaluates the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Atlassian maintains a risk and controls matrix within its GRC Tool.	Inspected the Atlassian GRC Tool to determine that the Atlassian Risk and Compliance team evaluated the design of controls and mitigation strategies during the period, including identifying risks and recommending changes in the control environment.	No exceptions noted.
		Inspected the Atlassian GRC Tool to determine that Atlassian maintained a risk and controls matrix within its GRC Tool.	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.		
VDR-1	Vendor agreements, including any security, availability, and confidentiality commitments, are reviewed during the procurement process.	Inspected contracts for a sample of critical vendors to determine that formal information sharing agreements were in place and included applicable confidentiality commitments.	No exceptions noted.
VDR-2	Atlassian reviews the SOC reports of its vendors on an annual basis.	Inspected SOC report review documentation for a sample of vendors to determine that SOC report reviews were performed during the period.	No exceptions noted.

Additional Criteria for Availability

Availability			
TSC Reference	**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.		
BBPL-29	**For Bitbucket Cloud:** Monitoring tools are in place to track and notify on the availability and reliability of Bitbucket Cloud systems and services.	**For Bitbucket Cloud:** Inspected the availability and reliability monitoring tools dashboard and alert configurations to determine that monitoring tools were in place to track and notify on the availability and reliability of Bitbucket Cloud systems and services.	No exceptions noted.
BBPL-31	**For Bitbucket Pipelines:** Monitoring tools are in place to track and notify on the availability and reliability of Bitbucket Pipelines services.	**For Bitbucket Pipelines:** Inspected the availability and reliability monitoring tools dashboard and alert configurations to determine that monitoring tools were in place to track and notify on the availability and reliability of Bitbucket Pipelines services.	No exceptions noted.
OG-13	**For Opsgenie:** Infrastructure and core service status are monitored continuously by AWS CloudWatch. If availability and processing capacity issues are detected in Opsgenie, alerts are sent to the on-call engineers.	**For Opsgenie:** Inspected system configurations to determine that infrastructure and core service status were monitored continuously by AWS CloudWatch.	No exceptions noted.
		For Opsgenie: Inspected alert configurations to determine that, if availability and processing capacity issues were detected in Opsgenie, alerts were sent to the on-call engineers.	No exceptions noted.

Availability			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
PL-14	**For Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Compass, Forge, Atlassian Analytics, Atlas, and Data Lake:** 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. Changes to availability are published online so that customers may check the status of the service.	**For Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Compass, Forge, Atlassian Analytics, Atlas, and Data Lake:** 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.
		For Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Compass, Forge, Atlassian Analytics, Atlas, and Data Lake: Inspected the Atlassian status page to determine that changes to availability were published online so that customers could check the status of the service.	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.		
BBPL-19	**For Bitbucket Cloud:** Bitbucket performs daily automated backups and annual restoration testing.	**For Bitbucket Cloud:** Inspected backup configurations to determine that Bitbucket performed daily automated backups.	No exceptions noted.
		For Bitbucket Cloud: Inspected the Bitbucket restoration test to determine that Bitbucket performed restoration testing during the period.	No exceptions noted.

Availability			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
BBPL-20	**For Bitbucket Pipelines:** Bitbucket Pipelines data is backed up daily and is subject to annual restoration testing.	**Bitbucket Pipelines:** Inspected the backup configurations for Bitbucket Pipelines to determine that Bitbucket Pipelines data was backed up daily.	No exceptions noted.
		Bitbucket Pipelines: Inspected the restoration test for Bitbucket Pipelines to determine that restoration testing was performed during the period.	No exceptions noted.
BBPL-23	**For Bitbucket Cloud:** Replication is monitored for failures, and an alert is created to be resolved.	**For Bitbucket Cloud:** Inspected system configurations and an example alert to determine that replication was monitored for failures and an alert was created to be resolved.	No exceptions noted.
BBPL-24	**For Bitbucket Cloud:** A formal disaster recovery plan is in place for Bitbucket and is tested annually.	**For Bitbucket Cloud:** Inspected the Bitbucket Cloud Disaster Recovery Plan to determine that a formal disaster recovery plan was in place for Bitbucket.	No exceptions noted.
		For Bitbucket Cloud: Inspected the disaster recovery plan test for Bitbucket to determine that the disaster recovery plan was tested during the period.	No exceptions noted.
DR-1	A disaster recovery policy is in place and is reviewed on an annual basis by the disaster recovery steering committee.	Inspected the disaster recovery policy and review documentation to determine that a disaster recovery policy is in place and is reviewed on an annual basis by the disaster recovery steering committee.	No exceptions noted.

Availability			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
ELC-17	Formal procedures are documented that outline the process the Company's staff follows to back up and recover customer data.	Inspected backup and recovery procedures to determine that formal procedures were documented that outlined the process the Company's staff followed to back up and recover customer data.	No exceptions noted.
OG-9	**For Opsgenie:** Opsgenie performs daily automatic backups, replication, and weekly restore testing.	**For Opsgenie:** Inspected the daily backup configurations for Opsgenie to determine that Opsgenie performed daily backups.	No exceptions noted.
		For Opsgenie: Inspected replication configurations for Opsgenie to determine that replication occurred automatically.	No exceptions noted.
		For Opsgenie: Inspected weekly restoration testing configurations for Opsgenie to determine that Opsgenie performed routine restore testing.	No exceptions noted.
PL-7	**For Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Compass, Atlassian Analytics, Atlas, and Data Lake:** Replication and backups are in place to provide data redundancy and availability for Micros. Data is automatically backed up hourly and routine restoration testing is performed annually.	**For Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Compass, Atlassian Analytics, Atlas, and Data Lake:** Inspected backup and replication configurations for in-scope systems to determine that hourly full backups were configured to provide redundancy and availability for Micros.	No exceptions noted.

Availability			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		For Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Forge, Compass, Atlassian Analytics, Atlas, and Data Lake: Inspected data restoration documentation to determine that testing was performed during the period.	No exceptions noted.
PL-8	**For JSM and Insight, and Bitbucket Pipelines:** Kubernetes clusters are replicated across multiple availability zones.	**For JSM and Insight, and Bitbucket Pipelines:** Inspected replication configurations to determine that Kubernetes clusters were replicated across multiple availability zones.	No exceptions noted.
PL-9	**For Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Opsgenie, Bitbucket Pipelines, Compass, Forge, Atlassian Analytics, Atlas, and Data Lake:** A formal disaster recovery plan is in place for Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Opsgenie, Bitbucket Pipelines, Compass, Forge, Atlassian Analytics, Atlas, and Data Lake, and it is tested quarterly.	**For Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Opsgenie, Bitbucket Pipelines, Compass, Forge, Atlassian Analytics, Atlas, and Data Lake:** Inspected the disaster recovery plan to determine that a documented disaster recovery plan was in place for Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Opsgenie, Bitbucket Pipelines, Compass, Forge, Atlassian Analytics, Atlas, and Data Lake.	No exceptions noted.
		For Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Opsgenie, Bitbucket Pipelines, Compass, Forge, Atlassian Analytics, Atlas, and Data Lake: Inspected results from the disaster recovery plan test for a sample of quarters to determine that testing was performed quarterly.	Exception noted. Atlassian Internal Audit identified that quarterly disaster recovery tests were performed for all in-scope services except Data Lake.

Availability			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.		
BBPL-24	**For Bitbucket Cloud:** A formal disaster recovery plan is in place for Bitbucket and is tested annually.	**For Bitbucket Cloud:** Inspected the Bitbucket Cloud Disaster Recovery Plan to determine that a formal disaster recovery plan was in place for Bitbucket.	No exceptions noted.
		For Bitbucket Cloud: Inspected the disaster recovery plan test for Bitbucket to determine that the disaster recovery plan was tested during the period.	No exceptions noted.
DR-1	A disaster recovery policy is in place and is reviewed on an annual basis by the disaster recovery steering committee.	Inspected the disaster recovery policy and review documentation to determine that a disaster recovery policy is in place and is reviewed on an annual basis by the disaster recovery steering committee.	No exceptions noted.
ELC-17	Formal procedures are documented that outline the process the Company's staff follows to back up and recover customer data.	Inspected backup and recovery procedures to determine that formal procedures were documented that outlined the process the Company's staff followed to back up and recover customer data.	No exceptions noted.
PL-9	**For Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Opsgenie, Bitbucket Pipelines, Compass, Forge, Atlassian Analytics, Atlas, and Data Lake:** A formal disaster recovery plan is in place for Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Opsgenie, Bitbucket Pipelines, Compass, Forge, Atlassian Analytics, Atlas, and Data Lake, and it is tested quarterly.	**For Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Opsgenie, Bitbucket Pipelines, Compass, Forge, Atlassian Analytics, Atlas, and Data Lake:** Inspected the disaster recovery plan to determine that a documented disaster recovery plan was in place for Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Opsgenie, Bitbucket Pipelines, Compass, Forge, Atlassian Analytics, Atlas, and Data Lake.	No exceptions noted.

Availability			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		For Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Opsgenie, Bitbucket Pipelines, Compass, Forge, Atlassian Analytics, Atlas, and Data Lake: Inspected results from the disaster recovery plan test for a sample of quarters to determine that testing was performed quarterly.	Exception noted. Atlassian Internal Audit identified that quarterly disaster recovery tests were performed for all in-scope services except Data Lake.

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.		
DS-1	Production data is not used in non-production environments and must be protected in alignment with Atlassian's System Acquisition, Development, and Maintenance Policy.	Inspected the System Acquisition, Development, and Maintenance Policy to determine that production data was prohibited by policy from being used or stored in non-production systems or environments.	No exceptions noted.
		Observed the test environment to determine that production data was not used in non-production systems or environments and was protected in alignment with Atlassian's System Acquisition, Development, and Maintenance policy.	No exceptions noted.
DS-2	An Information Classification Policy is in place to support the safety and security of Atlassian's data.	Inspected the Information Classification Policy to determine that a data classification policy was in place to support the safety and security of Atlassian's data.	No exceptions noted.
VDR-1	Vendor agreements, including any security, availability, and confidentiality commitments, are reviewed during the procurement process.	Inspected contracts for a sample of critical vendors to determine that formal information sharing agreements were in place and included applicable confidentiality commitments.	No exceptions noted.

Confidentiality			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.		
BBPL-1	**For Bitbucket Cloud, Bitbucket Pipelines, and Compass:** The removal of a customer's Bitbucket repository data occurs within seven days from the date the services are terminated.	**For Bitbucket Cloud, Bitbucket Pipelines, and Compass:** Inspected system configurations to determine that the removal of a customer's Bitbucket repository data was configured to occur within seven days from the date the services were terminated.	No exceptions noted.
OG-1	**For Opsgenie:** Opsgenie data is deleted within 30 days of receipt of a request for deletion.	**For Opsgenie:** Inspected system configurations to determine that Opsgenie customer data was configured to be automatically deleted within 30 days of receipt of request for deletion.	No exceptions noted.
PL-1	**For Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Data Lake, Atlassian Analytics, Atlas, and Forge:** Customer data is deleted from the Systems in a timely manner upon request or termination of the customer subscription.	**For Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Data Lake, Atlassian Analytics, Atlas, and Forge:** Inspected in-scope system configurations to determine that customer data was configured to be automatically deleted upon request or termination of the customer subscription in accordance with SLAs.	No exceptions noted.

Section 5

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

Management's Response to Testing Exceptions

Service Organization's Controls	Results of Tests	Management's Response
User awareness training is performed at least annually for employees and contractors as part of the Atlassian Security Awareness program.	Exceptions noted. For 3 of 44 employees and contractors sampled, user awareness training was not completed during the period.	Atlassian has confirmed the 3 sampled employees have either completed security training or are no longer employed by Atlassian.
For Bitbucket Cloud and Bitbucket Pipelines: Access to customer repositories by the Bitbucket internal support team is reviewed quarterly by the lead Support Engineer.	Exception noted. Atlassian Internal Audit identified that the quarterly access reviews did not include all user groups with access to Bitbucket and Bitbucket Pipelines customer repositories.	Atlassian has reviewed the missed user groups, ascertained that access to the customer repositories is appropriate, and has updated procedures to ensure completeness of future reviews. Additionally, user provisioning and access termination controls at the Active Directory level were deemed effective and served as compensating controls.
For Forge, Data Lake, Atlassian Analytics, Atlas, and JSM and Insight: User access reviews are performed semi-annually, and issues identified are remediated in a timely manner.	Exceptions noted. Atlassian Internal Audit identified that a user access review for Data Lake did not occur during the period.	Atlassian has reviewed the missed accounts, ascertained that access is appropriate, and has updated procedures to ensure completeness of future reviews. Additionally, user provisioning and access termination controls at the Active Directory level were deemed effective and served as compensating controls. This issue was identified proactively by Atlassian's internal audit team and has been remediated and validated.

Service Organization's Controls	Results of Tests	Management's Response
For Opsgenie: Access to customer data by the Opsgenie Support team is supported by a valid and approved customer support request.	Exception noted. Atlassian Internal Audit identified that an Opsgenie support member was able to continue accessing customer data without a valid customer support request.	Atlassian confirmed that the admin user was able to continue accessing customer data following consent withdrawal due to a platform migration causing a break in the functionality. Atlassian has since implemented a control to ensure that where customer data access is revoked the associated access token is expired and is no longer accessible by the admin. This issue was identified proactively by Atlassian's internal audit team and has been remediated and validated.
For Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Opsgenie, Bitbucket Pipelines, Compass, Forge, Atlassian Analytics, Atlas, and Data Lake: A formal disaster recovery plan is in place for Jira Cloud, JPD, Confluence Cloud, JSM and Insight, Opsgenie, Bitbucket Pipelines, Compass, Forge, Atlassian Analytics, Atlas, and Data Lake, and it is tested quarterly.	Exception noted. Atlassian Internal Audit identified that quarterly disaster recovery tests were performed for all in-scope services except Data Lake.	Atlassian has since updated the disaster recovery test procedures to ensure these two services are included in the regular disaster recovery testing cycle. Monitoring mechanisms have also been implemented to ensure disaster recovery testing for these services is completed within the allocated timelines and due dates. This issue was identified proactively by Atlassian's internal audit team and has been remediated and validated.