Jira | Confluence | Bitbucket | Bitbucket Pipelines | Opsgenie
Jira Service Management and Insight | Data Lake | Compass | Forge

Atlassian PTY Ltd.

System and Organization Controls (SOC) 2 Type 2 Report

Atlassian Platform Description of System Relevant to Security, Availability, and Confidentiality

For the period November 1, 2020 through September 30, 2021

With Independent Service Auditor’s Report
including Tests Performed and Results Thereof

Table of Contents
Atlassian Platform

SECTION I: ATLASSIAN'S MANAGEMENT ASSERTION FOR ATLASSIAN PLATFORM

ATLASSIAN

Atlassian's Management Assertion for Atlassian Platform

We have prepared the accompanying Atlassian Platform Description of System Relevant to Security, Availability, and Confidentiality (Description) of Atlassian PTY Ltd. (Service Organization or "Atlassian") in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (Description Criteria). The Description is intended to provide report users with information about the Atlassian Platform (System) that may be useful when assessing the risks arising from interactions with the System throughout the period November 1, 2020 to September 30, 2021, particularly information about system controls that the Service Organization has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria for security, availability, and confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

Atlassian uses Amazon Web Services ("AWS") to provide physical safeguards, environmental safeguards, infrastructure support and management, and storage services, and NTT Communications ("NTT") to provide colocation physical access and environmental protection. The Description includes only the controls of Atlassian and excludes controls of AWS and NTT. The Description also indicates that certain trust services criteria specified therein can be met only if AWS and NTT's controls assumed in the design of Atlassian's controls are suitably designed and operating effectively along with the related controls at AWS and NTT. The Description does not extend to controls of AWS and NTT.

The Description also indicates that certain trust services criteria specified in the Description can be met only if complementary user entity controls assumed in the design of Atlassian's controls are suitably designed and operating effectively, along with related controls at the Service Organization. The Description does not extend to controls of user entities.

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

a. The Description presents the System that was designed and implemented throughout the period November 1, 2020 to September 30, 2021 in accordance with the Description Criteria.

b. The controls stated in the Description were suitably designed to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated as described and if user entities applied the complementary user entity controls and AWS and NTT applied the controls assumed in the design of Atlassian's controls throughout the period November 1, 2020 to September 30, 2021.

c. The Atlassian controls stated in the Description operated effectively throughout the period November 1, 2020 to September 30, 2021 to achieve the service commitments and system requirements based on the applicable trust services criteria, if user entities applied the complementary user entity controls and AWS and NTT applied the controls assumed in the design of Atlassian's controls throughout the period November 1, 2020 to September 30, 2021.

DocuSigned by:

88C748362EA44C0...

Adrian Ludwig
Chief Trust Officer, Atlassian

Section II: Independent Service Auditor's Report

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

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

Independent Service Auditor's Report

To the Management of Atlassian PTY Ltd.

Scope

We have examined Atlassian's accompanying Atlassian Platform Description of System Relevant to Security, Availability, and Confidentiality of its Atlassian Platform systems used as a unified cloud technology platform that includes Atlassian's products and applications throughout the period November 1, 2020 to September 30, 2021 (Description) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (Description Criteria) and the suitability of the design and operating effectiveness of controls included in the Description throughout the period November 1, 2020 to September 30, 2021 to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria for security, availability, and confidentiality set forth in TSP section 100, 2017 *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

Atlassian uses Amazon Web Services ("AWS") to provide physical safeguards, environmental safeguards, infrastructure support and management, and storage services, and NTT Communications ("NTT") to provide colocation physical access and environmental protection. 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 the Atlassian Platform system; its controls; and the types of complementary subservice organization controls that the service organization assumes have been implemented, suitably designed, and operating effectively at AWS and NTT. Our examination did not extend to the services provided by AWS and NTT and we have not evaluated whether the controls management assumes have been implemented at AWS and NTT have been implemented or whether such controls were suitably designed and operating effectively throughout the period November 1, 2020 to September 30, 2021.

The Description also indicates that Atlassian's controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of Atlassian's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Atlassian'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 the service commitments and system requirements were achieved. Atlassian has provided the accompanying assertion titled, Atlassian's Management Assertion for Atlassian Platform (Assertion) about the presentation of the Description based on the Description Criteria and suitability of the design and operating effectiveness of the controls described therein to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria. Atlassian is responsible for (1) preparing the Description and Assertion; (2) the completeness, accuracy, and method of presentation of the Description and Assertion; (3) providing the services covered by the Description; (4) identifying the risks that would threaten the achievement of the service organization's service commitments and system requirements; and (5) designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve its service commitments and system requirements.

Service auditor's responsibilities

Our responsibility is to express an opinion on the presentation of the Description and on the suitability of the design and operating effectiveness of the controls described therein to achieve the Service Organization's service commitments and system requirements, based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the Description is presented in accordance with the Description Criteria, and (2) the controls described therein are suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we have 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
- performing procedures to obtain evidence about whether the controls stated in the Description are 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.
- assessing the risks that the Description is not presented in accordance with the Description Criteria and that the controls were not suitably designed or operating effectively based on the applicable trust services criteria.

- testing the operating effectiveness of those controls based on the applicable trust services criteria.
- evaluating the overall presentation of the Description.

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

Inherent limitations

The Description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to its own particular needs.

Because of their nature, controls at a service organization 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 evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls based on the applicable trust services criteria is subject to the risk that the system may change or that controls at a service organization may become ineffective.

Description of tests of controls

The specific controls we tested, and the nature, timing, and results of those tests are listed in the accompanying Atlassian's Controls and Service Auditor's Tests of Controls and Results of Tests (Description of Tests and Results).

Opinion

In our opinion, in all material respects:

a. the Description presents the Atlassian Platform system that was designed and implemented throughout the period November 1, 2020 to September 30, 2021 in accordance with the Description Criteria.

b. the controls stated in the Description were suitably designed to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria if the controls operated effectively and if AWS and NTT and user entities applied the controls assumed in the design of Atlassian's controls throughout the period November 1, 2020 to September 30, 2021.

c. the controls stated in the Description operated effectively to provide reasonable assurance that the service commitments and system requirements were achieved based on the applicable trust services criteria throughout the period November 1, 2020 to September 30, 2021, if AWS and NTT and user entity controls assumed in the design of Atlassian's controls operated effectively throughout the period November 1, 2020 to September 30, 2021.

Restricted use

This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of Atlassian, user entities of the Atlassian Platform systems during some or all of the period November 1, 2020 to September 30, 2021 and prospective user entities, independent auditors and practitioners providing services to such user entities 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, subservice organizations, or other parties, including complementary user entity controls and subservice organization controls assumed in the design of the service organization's controls
- Internal control and its limitations
- User entity responsibilities and how they interact with related controls at the service organization
- 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.

Ernst + Young LLP

December 9, 2021

Section III: Atlassian Platform Description of Systems Relevant to Security, Availability, and Confidentiality

Atlassian Platform Description of Systems Relevant to Security, Availability, and Confidentiality

Scope and Purpose of the Report

This report describes the control structure of Atlassian PTY Ltd. (hereinafter "Atlassian" or "company") as it relates to its Atlassian Platform that includes Jira Cloud, Confluence Cloud, Opsgenie, Jira Service Management and Insight, Bitbucket Cloud, Bitbucket Pipelines, Data Lake, Forge, and Compass systems (hereinafter "the Systems") for the period from November 1, 2020 to September 30, 2021 for the Security, Availability, and Confidentiality Trust Services Criteria.

The description is intended to provide the Atlassian Platform's customers, prospective customers, and auditors with information about the system controls related to the criteria for the Security, Availability, and Confidentiality Trust Services Criteria set forth in the Description Criteria DC section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* ("Description Criteria") and the suitability of the design and operating effectiveness of the controls included in the Description throughout the period from November 1, 2020 to September 30, 2021 to provide reasonable assurance that Atlassian's service commitments and system requirements would be achieved based on the trust services criteria for security, availability, and confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust criteria). This description may not provide information about Atlassian's systems controls that do not relate to the Applicable Trust Services Criteria.

Company Overview and Background

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). Additionally, Atlassian embraces distributed teamwork, enabling employees who are currently remotely working 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.

The systems in-scope for this report are the Systems hosted at Amazon Web Services ("AWS") and NTT Communications ("NTT") datacenter, and the supporting 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 Service

Jira and Confluence Cloud

Jira and Confluence Cloud is a Software as a Service ("SaaS") solution which covers the Jira Suite (Jira Software and Jira Core) and Confluence. The Jira family of products are 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 at high velocity, so they can respond to business changes and deliver great customer and employee experiences fast.

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.

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.

Bitbucket Cloud

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

Bitbucket Cloud's services are hosted in AWS data centers, using the AWS infrastructure as a service offering ("IaaS"). These services were fully migrated over from the NTT data center in Ashburn, Virginia, where they were hosted from November 1, 2020 to August 26, 2021. Procedures exist to monitor completeness and accuracy of customer data migrated from NTT data center in Ashburn (ASH2) to the Micros platform hosted in AWS.

Bitbucket Pipelines

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

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 (not in-scope).

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.

Compass

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

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, Jira Service Management and Insight, Bitbucket Cloud, Bitbucket Pipelines, Data Lake, Forge, and Compass systems (hereinafter "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 system.

Security, availability, and confidentiality commitments to user entities are documented and communicated in the terms of services within the sign-up page in the Systems and through the Master Service Agreement ("MSA") with other vendors and enterprise customers. The description of the service offering and the system delineating the boundaries and describing relevant components is documented on the Atlassian intranet and the customer-facing website. Security, availability, and confidentiality commitments are standardized and communicated to its customers via the Atlassian Trust Security Page. The security, availability, and confidentiality commitments include, but are not limited to, the following:

- Operational Practices – A range of security and confidentiality controls designed to address the security and confidentiality criteria of the Atlassian Platform. Such security and confidentiality controls include permitting and restricting system users to access customer data and the information they need based on their roles and responsibilities, while restricting them from accessing information not needed for their role.
- Product Security – A range of security controls Atlassian implements to keep the 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, as well as optimal performance with redundancy and failover options globally while maintaining multiple locations and availability zones across AWS regions.
- Security Process – A range of vulnerability and security processes to detect security and vulnerability issues, which allows Atlassian to address identified gaps as soon as possible to minimize impact.

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

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:

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 & Confluence Cloud	✓			✓	✓	✓	✓	✓
Jira Service Management and Insight	✓	✓		✓	✓	✓	✓	✓
Opsgenie*		✓		✓	✓	✓		
Jira Service Management (inc. Insight)	✓			✓	✓	✓	✓	✓
Bitbucket Cloud** (Pre-Migration)	✓		✓	✓				
Bitbucket Cloud (Post-Migration)	✓		✓	✓	✓	✓	✓	✓
Bitbucket Pipelines	✓			✓	✓	✓	✓	✓
Data Lake	✓				✓		✓	✓
Forge				✓				
Compass	✓			✓	✓	✓	✓	✓

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

** Prior to migration, Bitbucket Cloud's services and features are provided by a set of services running in the NTT data center in Ashburn, Virginia, with backup services on standby in the NTT data center in Santa Clara, California.

Network

Jira Cloud, Confluence Cloud, JSM and Insight, and Compass

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

All these DNS names resolve to a wildcard record under *.atlassian.net (or *.Jira.com). The DNS response is latency-based (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 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 another AWS region than the one the proxy is located in. 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 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 TLS.

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 Route53 for geolocation reference. Route53 logic will then route requests to the appropriate vTM host which terminates TLS.

User-initiated connections in Bitbucket Cloud are available using IPv4 or IPv6 addresses and are available on TCP ports 22 (SSH), 80 (HTTP) or 443 (HTTPS). A special hostname, altssh.Bitbucket.org, provides SSH connectivity over port 443 for users whose networks restrict outbound connections to port 22.

Within the data center, Bitbucket Cloud systems used logical binding on multiple network interfaces to provide redundancy against hardware failures. A dedicated VLAN connected application nodes to repository storage; other VLANs connected application nodes, load balancers, database servers and other resources to each other. All internal resources were isolated from the Internet by the firewall.

Data Lake

Direct access to Data Lake is not provided, however, access to data is gained via a customer's chosen Business Intelligence (BI) tool via Cloud API token. Data Lake data is encrypted in transit via HTTPS connection and valid 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.

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

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 the proxy is located in.

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.

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, Opsgenie, Bitbucket Cloud (Post-Migration), Bitbucket Pipelines, Data Lake, and Compass

AWS provides infrastructure as a service ("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.

Bitbucket Cloud (Pre-Migration)

Application nodes are stateless and clustered based on their primary service. Cluster types include, but are not limited to, the user interface; API; Git repository operations over SSH; Git repository operations over HTTP; asynchronous tasks. Physical server configurations are managed using various tools including Puppet.

Forge

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

One or more Forge shard 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 AWS Lambda runs in multiple availability zones in a single region.

The Forge management code runs on 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 availability zones 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, and Compass

The above-mentioned products use logically separate Amazon Relational Database Service (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 availability zone within the same AWS region to mitigate the risk of data loss due to hardware failure.

Database logs are kept for at least 24 hours and 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 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 a DynamoDB, which relates the customer to its respective data store.

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

Opsgenie

Opsgenie's primary datastore is AWS DynamoDB, which is hosted by AWS and managed by Opsgenie. AWS DynamoDB 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.

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

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

Bitbucket Cloud (Pre-Migration)

Customer data was stored in a PostgreSQL database. PostgreSQL contained account attributes, permissions, issues, pull requests and wiki data.

Bitbucket Cloud (Post-Migration)

Bitbucket Cloud uses a single shared Aurora database for all customers. The database server has multiple independent synchronous replicas in multiple availability zones within the same AWS region to mitigate the risk of data loss due to hardware failure. Database logs are kept for at least 24 hours and backups are kept for 30 days as redundancy, to allow restoration of data within a reasonable point in time, if needed.

Attachments stored in 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 DynamoDB, which relates the customer to the attachment stored in Amazon S3.

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

Bitbucket Pipelines

Bitbucket Pipelines' primary data storage utilizes DynamoDB, which is hosted by AWS and managed by Atlassian. AWS DynamoDB is highly available, scalable, and spans multiple data centers and regions. Amazon Elasticsearch is used to index DynamoDB tables using a custom *indexer sidecar*, which listens on each DynamoDB'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.

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/views in their own namespace, using table Access Control Lists (ACLs) to prevent cross-contamination and restrict visibility of data.

Forge

Forge app metadata is stored in multiple Amazon Relational Database Service (RDS) databases, each having an independent synchronous replica in a different availability zone within the same AWS region to mitigate the risk of data loss due to hardware failure. Database logs are kept for at least 24 hours and backups are kept for 30 days as redundancy, to allow point-in-time recovery (PITR) of data. Amazon Simple Storage Service (S3) is used to store backups and log archives, providing high durability and availability and is the operational responsibility of AWS.

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

Forge apps may store app data with the Forge storage API, providing a key value datastore backed by AWS DynamoDB.

Compass

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

DynamoDB 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 DynamoDB.

Provisioning Architecture

Jira Cloud, Confluence Cloud, JSM and Insight, Opsgenie, Bitbucket Cloud, Bitbucket Pipelines, Data Lake, Forge and Compass

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 are 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 Systems:

Component	Service Provider	Products
Hosting Systems	Amazon EC2	Jira Cloud, Confluence Cloud, JSM and Insight, Opsgenie, Bitbucket Cloud (Post-Migration), Bitbucket Pipelines, Data Lake, Forge, and Compass
	Kubernetes on top of EC2	Insight and Pipelines
	CentOS	Bitbucket Cloud (Pre-Migration), Compass
	NTT Data Center	Bitbucket Cloud (Pre-Migration)
	AWS Lambda	Forge
Storage and Database	Amazon Relational Database Service (RDS) for PostgreSQL	Jira Cloud, Confluence Cloud, JSM and Insight, Bitbucket Cloud (Pre-Migration), Forge, and Compass
	Amazon DynamoDB	Jira Cloud, Confluence Cloud, JSM, Opsgenie, Bitbucket Cloud (Post-Migration), Bitbucket Pipelines, Forge, and Compass
	Amazon Simple Storage Service (S3)	Jira Cloud, Confluence Cloud, JSM and Insight, Opsgenie, Bitbucket Cloud (Post-Migration), Compass, Bitbucket Pipelines, Data Lake, Forge
	Amazon Aurora	Opsgenie, Forge, and Bitbucket Cloud (Post-Migration)
	Amazon Key Management Service (KMS)	Opsgenie
	NetApp CVS	Bitbucket Cloud (Pre-Migration and Post-Migration)

Component	Service Provider	Products
	Redis	Opsgenie, Bitbucket Cloud (Pre-Migration), Bitbucket Pipelines, and Forge
	Databricks Workspaces	Data Lake
Network	Amazon Virtual Private Cloud (VPC)	Jira Cloud, Confluence Cloud, JSM and Insight, Bitbucket Cloud (Post-Migration), Opsgenie, Compass, Bitbucket Pipelines, Forge
	Amazon Load Balancers (ALB)	Jira Cloud, Confluence Cloud, JSM and Insight, Opsgenie, Bitbucket Cloud (Post-Migration), Bitbucket Pipelines, Forge, and Compass
	Corporate firewall	Jira Cloud, Confluence Cloud, JSM and Insight, Opsgenie, Bitbucket Cloud, Bitbucket Pipelines, Forge, and Compass
	Amazon CloudFront	Jira Cloud, Confluence Cloud, JSM and Insight, Bitbucket Cloud (Post-Migration), Opsgenie, Bitbucket Pipelines, Forge, and Compass
	Amazon Web Application Firewall (WAF)	Opsgenie, Insight, and Forge
	Kubernetes	Opsgenie
	Akamai	Bitbucket Cloud (Pre-Migration)
	Brocade Virtual Traffic Manager (vTM)	Bitbucket Cloud (Pre-Migration)
Application Cache	AWS ElastiCache	Jira Cloud, Confluence Cloud, JSM, Bitbucket Cloud (Post-Migration), and Compass
	Redis	Opsgenie, Bitbucket Cloud (Pre-Migration), Bitbucket Pipelines, Forge
Search & Analytics	Amazon Elasticsearch	Jira Cloud, Confluence Cloud, JSM and Insight, Opsgenie, Bitbucket Pipelines, and Compass

Component	Service Provider	Products
Messaging	Amazon Simple Queue Service (SQS)	Jira Cloud, Confluence Cloud, JSM, Compass, Bitbucket Pipelines, Forge, and Opsgenie
	Kinesis	Opsgenie and Forge
	Amazon Simple Notification Service (SNS)	Opsgenie and Bitbucket Pipelines
Build, Release, and Continuous Integration Systems	Bitbucket Cloud	Jira Cloud, Confluence Cloud, JSM and Insight, Opsgenie, Bitbucket Cloud, Bitbucket Pipelines, Forge, and Compass
	Deployment Bamboo	Jira Cloud, Confluence Cloud, JSM, Bitbucket Cloud (Pre-Migration)
	Bitbucket Pipelines	Bitbucket Cloud (Pre-Migration and Post-Migration), Insight, Bitbucket Pipelines, Forge, and Compass
Access Management	Active Directory	Jira Cloud, Confluence Cloud, JSM and Insight, Opsgenie, Bitbucket Cloud (Pre-Migration and Post-Migration), Bitbucket Pipelines, Forge, and Compass
	CyberArk (formerly Idaptive) Single Sign On (SSO)	Jira Cloud, Confluence Cloud, JSM and Insight, Opsgenie, Bitbucket Cloud (Pre-Migration and Post-Migration), Bitbucket Pipelines, Forge, and Compass
	Duo Two-factor authentication (2FA)	Jira Cloud, Confluence Cloud, JSM and Insight, Opsgenie, Bitbucket Cloud (Pre-Migration and Post-Migration), Bitbucket Pipelines, Forge, and Compass
Monitoring and Alerting	Splunk	Jira Cloud, Confluence Cloud, JSM and Insight, Opsgenie, Bitbucket Cloud (Pre-Migration and Post-Migration), Bitbucket Pipelines, Forge, and Compass
	SignalFX	Jira Cloud, Confluence Cloud, JSM and Insight, Opsgenie, Bitbucket

Component	Service Provider	Products
		Cloud (Pre-Migration and Post-Migration), Bitbucket Pipelines, Forge, and Compass
	Opsgenie	Jira Cloud, Confluence Cloud, JSM and Insight, Opsgenie, Bitbucket Cloud (Pre-Migration and Post-Migration), Bitbucket Pipelines, Forge, and Compass
	NewRelic	Bitbucket Cloud (Post-Migration) and Opsgenie
Customer Support and Communication	Intercom	Opsgenie
	Statuspage	Jira Cloud, Confluence Cloud, JSM, Opsgenie, Bitbucket Cloud, Bitbucket Cloud (Pre-Migration and Post-Migration), Bitbucket Pipelines, Forge
Vulnerability Scanning	Nexpose	Jira Cloud, Confluence Cloud, JSM and Insight, Opsgenie, Bitbucket Cloud (Pre-Migration and Post-Migration), Bitbucket Pipelines, Forge, and Compass
	Cloud Conformity	Jira Cloud, Confluence Cloud, JSM and Insight, Opsgenie, Bitbucket Cloud (Pre-Migration and Post-Migration), Bitbucket Pipelines, Forge, and Compass
	SourceClear	Jira Cloud, Confluence Cloud, JSM and Insight, Opsgenie, Bitbucket Cloud (Pre-Migration and Post-Migration), Bitbucket Pipelines, Forge, and Compass
Human Resource	Workday	Jira Cloud, Confluence Cloud, JSM and Insight, Opsgenie, Bitbucket Cloud (Pre-Migration and Post-Migration), Bitbucket Pipelines, Forge, and Compass
	Lever	Jira Cloud, Confluence Cloud, JSM and Insight, Opsgenie, Bitbucket Cloud (Pre-Migration and Post-

Component	Service Provider	Products
		Migration), Bitbucket Pipelines, Forge, and Compass
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. NTT Communications ("NTT") is a third-party vendor that provides colocation physical access and environmental protection. Atlassian has identified the complementary subservice organization controls of AWS and NTT to achieve the applicable trust services criteria. The other third-party vendors mentioned above are only applicable to support certain controls and criteria.

Organizational Structure

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

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

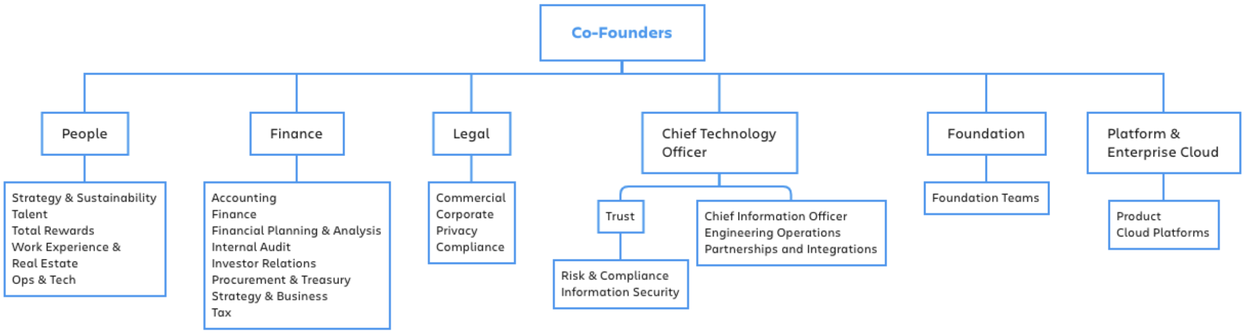

Figure 2: Atlassian's Organizational Chart

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:

- Platform and Enterprise Cloud— focuses on validating the demands of customers, provides insight and guidance around minimum viable product and user experience.
- People (in partnership with the people leaders) — focuses on determining the right talent strategy to deliver against the needs of Atlassian. People team is responsible for talent acquisition and learning, total rewards and technology, and workplace experiences.
- Foundation — exists to harness the resources of Atlassian to champion organizations who believe that education is the key to eliminating disadvantage. This is accomplished by improving educational outcomes in developing countries, increasing skill-based volunteering, and leveraging Atlassian's products.
- Legal — responsible for matters related to corporate development, privacy, general counsel operations, and public relations.
- Finance — responsible for handling finance and accounting.
- Chief Technology Officer (Technology Operations) — oversees Engineering, Trust, Risk and Compliance, Information Security, Mobile, Ecosystem and Platform.

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 outlined business objectives.
- showing commitment to meet regulatory obligations.
- focused on continual iteration and improvement.
- provided for an exception process.
- supported by the Policy Framework and Structure.

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

Item	Defines	Explanation
Policy	General rules and requirements ("state")	Outlines specific requirements or rules that must be met.
Standard	Specific details ("what")	Collection of system-specific or procedural-specific requirements that must be met by everyone.
Guideline	Common practice, recommendations, and suggestions	Collection of system specific or procedural specific "suggestions" for best practice. They are not requirements to be met but are strongly recommended. Effective policies make frequent

Item	Defines	Explanation
		references to standards and guidelines that exist within an organization.
Standard operating procedures	Steps to achieve Standard/Guideline requirements, in accordance with the rules ("actions")	Positioned underneath a standard or guidelines, it is a set of instructions on how to accomplish a task. From a compliance perspective, a procedure is also referred to as "Control Activity". The goal of a process/procedure is to help achieve a consistent outcome defined by the Standard or Guideline.

Policy Requirements

Every policy has a Policy Owner who is responsible for managing the risk outlined in the Policy Objective. All policies are reviewed, at least annually, to help ensure they are relevant and appropriately manage risk in accordance with Atlassian's risk appetite. Changes are reviewed by the Atlassian Policy Committee (“APC”) and approved by the corresponding Policy Owner.

Policy exceptions and violations are also reviewed by the APC and actions are recommended to the Policy Owners and executive team. Policy owners can approve exceptions for a period no longer than one year.

Policy Review Process

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

Relevant Aspects of the Control Environment, Risk Assessment, Control Activity, Monitoring, and Information and Communication

Control Environment

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

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

Atlassian’s Board of Directors and various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) meet at least annually to review committee charters and corporate governance, which defines their roles, responsibilities, member qualifications, meeting frequency, and other discussion topics. Meeting minutes of the annual meetings are recorded, which include participants and 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 down into each of the product groups for execution by the Management Team. Progress toward targets is evaluated at least quarterly by the Executive and Management Teams.

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

Management Controls and Operating Style

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

- Standards — Atlassian follows specific standards that enable the organization to exercise practices around security, availability, quality, reliability, and confidentiality.
- Tools — Atlassian leverages tools designed specifically to assist in identifying, analyzing, tracking, deciding, implementing, and monitoring risks and findings. In addition, the tools allow the company to effectively communicate and collaborate using workflows to help ensure activities are properly tracked. The use of customized tools allows them to be more closely integrated with the standard way of how Atlassian operates: specific, scalable, systematic, and robust.
- Enterprise Risk Management Process — Atlassian uses an Enterprise Risk Management process that is modeled after 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 more effectively establish a controlled environment.

Integrity, Ethical Values and Competence

The integrity, ethical values and competence are key elements of Atlassian's control environment. Atlassian employees are required to acknowledge the Code of Conduct, Insider Trading Policy, FCPA, and Anti-Corruption Policy. The HR Operations team is involved in reviewing and monitoring that these policies and agreements are acknowledged, and background screening is followed through in a timely manner. Employees and contractors with access to Atlassian systems are asked to re-acknowledge on an annual basis.

Learning and Development

Atlassian requires its employees to complete anti-harassment training and offers opportunities for technical training and professional development. In regard to technical training and professional development, every Atlassian employee has the ability to reach their fullest potential and do the best work of their lives by providing 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 one's 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 extensive research to map formalized competencies to the majority of roles at Atlassian, particularly those that are customer and product facing. Managers and employees use these competencies to see what is required for success in a position and what areas an employee needs further development/training around. Based on these gaps, managers and the Learning and Development team can recommend training, self-study, or coaching as needed.
- Degreed, Get Abstract, LinkedIn Learning, Learndot, and Intellum are extensive third-party tools Atlassian uses to access thousands of online learning resources for free. It also serves 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.

Human Resource Policies and Procedures

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

The recruiting process is based on prior relevant experience, educational background, and a clear understanding of integrity and ethical behavior. As part of the hiring process, interview feedback is collected in the applicant tracking system, Lever, for all candidates that participate in an onsite interview. Each interviewer, hiring manager, and HR member has access to Lever, and is able to view the candidates' profile. A recruiter will not initiate an offer for hire without receiving a minimum of 1 interview review in Lever prior to their start date. The exception to this process is contractors, interns, and graduates. For contractors, who are hired outside of the standard hiring process and outside of Lever, there is a confirmation screening step in the on-boarding process within the Service Desk. For interns and graduates, a recruiting manager will approve the offer letters because of the bulk nature and timing of these hires.

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

Risk Assessment

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 Enterprise Risk Management (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/department/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 in the course of 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 organizations. 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 period, Atlassian performs a number of periodic and ad-hoc assessments, which includes key product stakeholders. Results of the assessments are captured in the Atlassian Governance, Risk and Compliance ("GRC") tool.
- Incidents — Atlassian utilizes a common Incident Management Process ("IM"), including Post Incident Review ("PIR"). The goal of PIR is not only to establish the root cause but also to create actions aimed at reducing the risk of repeated incidents.
- Organizational policies — Organizational policies that have been put in place to achieve the organization's strategic goals and objectives.
- Interviews with major stakeholders and subject matter experts ("SME") — As part of the structured Enterprise Risk Assessment Atlassian interviews all members of the Management team and engages with SMEs as needed.
- Other sources — Atlassian may consult industry publications, analyses, incidents, etc., as necessary.
- Internal and external context of the ERM process includes but is not limited to understanding:
  - Competitive environment — who are Atlassian's major competitors, what threat level they present, what are the trends in Atlassian's industry
  - Legal/Regulatory environment — what are Atlassian's obligations within their operating jurisdictions, what are the industry standards Atlassian needs to abide by
  - Financial environment — current status as well as trends in the financial and currency markets that could affect us, perceptions, 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, what is the perception of Atlassian and its products/services, 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 us, what are the current status and trends of the talent pools where Atlassian currently has or plans to establish presence
  - Natural environment — considerations related to natural disasters, and office locations and facilities

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

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

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

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

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

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

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

The Atlassian Risk and Compliance team monitors the internal control environment and identifies significant changes that have occurred. The Risk and Compliance team meets on a monthly basis with bi-annual strategic planning to discuss:

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

Entity Level and Financial 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 Enterprise Risk Management ("ERM"). The results are included with the enterprise risk assessment which is communicated to the board and executive level managers annually.

A whistleblower hotline is established and is accessible to both external individuals and employees within the Company. The whistleblower hotline is included within the Code of Conduct which all employees are required to certify that they received. If an individual calls the Whistleblower hotline the General Counsel, Associate General Counsel and Audit Committee Chair receives 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.

The Corporate Controller reviews the financials and footnote disclosures prepared by the member of Technical Accounting for reasonableness, internal consistency and confirms prior period balances of the final financial statements. A copy of the reviewed statements is attached to an email to the Chief Financial Officer evidencing completion of review.

The Spend Authority Limits (Signature Authority Matrix) is maintained by Legal which establishes the signature authority for expenditures, contracts, capital acquisitions, and write offs. The Limits are reviewed annually at every Board of Directors meeting.

On an annual basis, the Head of Finance and Accounting reviews the financial statement risk assessments based on knowledge of the Company and also against the assumptions used in the prior year. The reviewer also ensures that the total net profit and loss amount is within the financial risk assessments and ties to the fiscal year-end financial statements. Materiality threshold and methodology are also reviewed and compared with other companies to determine the appropriateness of materiality.

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 subject matters experts ("SMEs"). This involves evaluating the supplier's control environment and overall security posture based on information contained in supplier questionnaires, compliance reporting (e.g., SOC2), and policies. Vendor agreements, including terms and conditions, 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 & 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.

Internal and External Audit

The Internal Audit team conducts internal audits relating to Sarbanes-Oxley 404 (SOX), Service Organization Control (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.

Information and Communication

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

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

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

Atlassian uses the Atlassian Trust Center website to communicate the latest information on the security, reliability, privacy, 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:

- 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 forms
- 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. Availability of the Systems, including the status and uptime, is published in the customer facing website for all customers.

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, privacy violation, legal liability, and natural disaster.

Information Security Controls

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

Periodic Review of Risks and Controls

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

Information Security Training

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

All Atlassian employees (including contractors) are subject to mandatory Security 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.

Description of Control Activities and Relevant Aspects of Operations

A. Change Management

Change initiation

Changes to the Systems and their supporting utilities and services are planned by the product development teams, which includes 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, creating DNS records, etc.

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. 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 products’ 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. Additionally, audit logs are periodically reviewed to identify potential unauthorized changes.

Scanning of Production Code

The Systems utilize SourceClear to regularly scan and review the code base to detect vulnerable open-source libraries being used. The goal is for Atlassian to move completely off of SourceClear and primarily use Snyk by the end of the calendar year 2021. 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 periodically 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 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.

B. Logical Access

Provisioning Customer Production Accounts

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

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

<u>Jira Cloud, Confluence Cloud, JSM and Insight, Data Lake, and Compass</u>

After acknowledging the customer agreement, the customer's order is accepted and provisioned. Dedicated databases for the customer product instances are created in AWS 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, as well as the associated databases. After successful provisioning, the customer's configuration information is stored in the Catalogue Service ("CS"). CS stores the master copy of the customers' configuration information (e.g. database location), which is then fed into Tenant Context Service ("TCS") for fast 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 DynamoDB 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, accounts.

Bitbucket Cloud (Pre-Migration and Post-Migration) 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 was created in PostgreSQL (Aurora DB post migration) and NetApp through the use of unique identifiers. Once a repository was created in Bitbucket Cloud, it created 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 a number of 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 catalogue service ("CS"). CS stores the master copy of customer configuration information such as database location, which is then fed into the tenant context service ("TCS") for fast 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

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

De-provisioning Customer Production Accounts

Jira Cloud, Confluence Cloud, JSM and Insight, Data Lake, Forge, and Compass

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 are able to 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 safely, consistently, and automatically.

Bitbucket Cloud (Pre-Migration and Post-Migration) 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 have the ability to add and remove user accounts. Users can only access instances they are authorized to.

Jira Cloud, Confluence Cloud, JSM and Insight, 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 Tenant Context Service ("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, licensing information, etc. The application validates the login session for the user and responds to the request. If the session is not present or not valid, the user is redirected back to the original login system. During the login process, the application verifies whether the user is authorized to access the requested products. If verification passes, a valid session is created, and the user is routed to the requested products. For users who are not authorized, the request is denied. Mobile applications access the 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).

Opsgenie

Users can access Opsgenie via the browser user interface and mobile apps. 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 admins. Team admins 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.

Bitbucket Cloud (Pre-Migration)

Users can access Bitbucket Cloud via the browser user interface, directly from the command line using SSH or HTTPS, or using Bitbucket Cloud's REST API.

Users can authorize external services to access data using OAuth 2 and Atlassian's Connect framework (application specific passwords). Users can also configure Bitbucket Cloud to send email and webhook notifications based on changes to the code stored on Bitbucket Cloud.

Bitbucket Cloud (Post-Migration) and Bitbucket Pipelines

Access is gained via a typical HTTPS connection to the vTM load balancers, 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 as the vTM cannot terminate SSL.

Data Lake

Customer access is not direct but leverages a Cloud API token through the customer's chosen Business Intelligence (BI) tool. This token is verified to be associated with the correct permissions for this organization, and then translated into customer identity which 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 apps within the Forge Developer platform.

If developing on the Atlassian platform, the user is directed to acknowledge the standardized Atlassian Developer Terms, which defines 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 App User

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

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, Bitbucket Cloud (Pre-Migration and Post-Migration), Bitbucket Pipelines, Data Lake, Forge and Compass

The password settings for customers, of the above-mentioned products, are governed through password complexity, in which lowercase, uppercase, numbers, as well as symbols are used. The default password policy for external users requires a minimum of 8 characters with no hard expiry.

It is the customers' responsibility to ensure that their accounts are appropriately configured and set up to their corporate network/password and other authentication mechanisms such as Single Sign-On ("SSO") or two-factor authentication.

Opsgenie

Opsgenie customers are governed with a trial account when they first sign up. It is the customers' responsibility to ensure that their accounts are appropriately configured with Single Sign-On ("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 ensure that only approved individuals can access these systems and assets.

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

Duo two-factor authentication is also required when logging into 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

Atlassian Internal User Provisioning

Jira Cloud, Confluence Cloud, JSM and Insight, Opsgenie, Bitbucket Cloud (Pre-Migration and Post-Migration), Bitbucket Pipelines, Data Lake, Forge and Compass

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

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

- Each Atlassian user account must have an Active Directory account
- Each Atlassian user account must be a member of the appropriate 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.

Bitbucket Cloud (Pre-Migration)

Direct access to PostgreSQL DB and CentOS is approved prior to granting access. Access to CentOS requires SSH and LDAP, and access to PostgreSQL DB requires SSH and a username and password. Access to the CentOS system hosting the Bitbucket Cloud application is provisioned via LDAP along with SSH keys. A valid SSH key is granted upon appropriate approval and the Bitbucket Cloud Operations team is responsible to help ensure the access is appropriate and only members of appropriate teams are provisioned access. Databases such as PostgreSQL are provisioned by the Bitbucket Cloud Operations team on an individual basis.

Atlassian Internal User De-provisioning

Deprovisioning of access via terminations is initiated at the Workday level. Human Resources 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 up to 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 are manually revoked.

Atlassian Internal User Role Changes

Role changes are a common practice and Atlassian has a process in place to make any internal transition an effortless and seamless event. When a user changes roles and moves from the Engineering, Support, or Finance group to one of the other areas (Engineering, Support, or Finance groups), an alert is generated and a notification is sent to the Human Resource 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/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 over Workday admin users on a semi-annual basis.

Access of Atlassian Support Team to User Data

Jira Cloud, Confluence Cloud, JSM and Insight, Bitbucket Cloud (Pre-Migration and Post-Migration), Bitbucket Pipelines, Data Lake, Forge, and Compass

Atlassian has a dedicated group of customer support personnel (known as Customer Support and Success or "CSS") who help customers troubleshoot issues during the course of using the above-mentioned products. Customer Support personnel are able to access customers' instances for a defined temporary period of time, 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 admin panel. Customer Support is able to define the consent duration required for access. The maximum amount of time for access is 7 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 have the ability to withdraw the consent approval before the given consent duration expiry.

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") timeframes. The Vulnerability Funnel automation notifies the appropriate system or application owner of new security vulnerabilities, sends multiple notifications as the vulnerability approaches its due date, and reports on issues not remediated by the due date to leadership.

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

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

Regular reviews of all identified Atlassian critical vulnerabilities are conducted daily when applicable and subject matter experts 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/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 which 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, etc.). In order to access the production environments, users must be authenticated to the Atlassian network (via the corporate office network or VPN) and therefore, enforcing protection by the firewalls.

Firewall rules are in place to restrict access to the production environment and only 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 protocol. Atlassian monitors the certificate authority issued TLS certificates and renews them prior to expiry.

C. Physical Access

Jira Cloud, Confluence Cloud, JSM and Insight, Opsgenie, Bitbucket Cloud, Bitbucket Pipelines, Data Lake, Forge, and Compass

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.

Bitbucket Cloud (Pre-Migration)

Prior to AWS migration, Bitbucket Cloud was hosted within NTT facilities. Atlassian reviewed the NTT 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 were followed-up and addressed as necessary.

Measures were taken to help ensure that staff who require physical access to Bitbucket Cloud servers were authorized and appropriate. All access requests were captured within an issue tracking system, reviewed, and approved as appropriate. Physical access to the data center was also reviewed on a regular basis.

D. 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.

E. Backup and Replication

Jira Cloud, Confluence Cloud, JSM and Insight, Bitbucket Cloud, and Forge

Atlassian employs Amazon Relational Database Services (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 DB instances using multiple Availability Zone (Multi-AZ) deployments, automatically provisioning, and maintaining a synchronous standby replica in a different Availability Zone 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 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 S3 backed up using versioning functionality. On an annual basis, backups are tested to ensure recoverability.

Opsgenie

Opsgenie uses AWS fully managed database services (DynamoDB, S3, and KMS) for storing and processing data. These services span multiple zones, with zones running master nodes isolated from each other. AWS seamlessly 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, RDS, and Elasticsearch), with Multi-AZ replication capability. Unlike the serverless approach, Opsgenie is responsible for configuring a number of zones, instances, and replication, while AWS is responsible for the physical server management. AWS provides automatic failover, but Opsgenie is able to initiate zone-based failovers as well. Opsgenie ensures appropriate replication setup and configuration of these zones, and continuously monitors their replication.

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 is down. As such, Opsgenie's infrastructure and backup is replicated on a continuous basis using AWS.

Bitbucket Cloud (Pre-Migration)

All primary database servers resided in Atlassian's physical data centers with replication nodes and backups stored in both physical data centers. Production data was constantly replicated (in near real-time or at most within four hours) between the read-write instance and multiple read-replicas hosted in Ashburn, VA, and Santa Clara, CA.

User data stored on file systems were managed by Atlassian's network filers, which only existed in these data centers. Data was replicated from the primary data center to the DR data center at all times via NetApp's proprietary mirroring technology. Bitbucket Cloud production data in NetApp was also replicated every two hours (lagging on average from 10-20 minutes and at most within four hours) from its primary site to a secondary site. Customer data stored in PostgreSQL was automatically backed up daily, and backups tested annually to ensure recoverability.

The replication of Bitbucket Cloud production data was monitored for failures and an alert was created and resolved based on Atlassian's incident management process.

Bitbucket Cloud (Post-Migration)

Amazon RDS Aurora (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 the 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 DynamoDB, managed by the internal PaaS, and protecting tables from accidental write or delete operations through point-in-time recovery (PITR). In the event that 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.

Data Lake

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

Compass

DynamoDB and Elasticsearch provide high availability and failover support for DB instances using multiple Availability Zone (Multi-AZ) deployments, automatically provisioning, and maintaining a synchronous standby replica in a different Availability Zone 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 DynamoDB, managed by the internal PaaS, and protecting tables from accidental write or delete operations through point-in-time recovery (PITR). In the event that 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 kept at all times and expire after 14 days.

In addition to automated snapshots, the internal PaaS platform takes hourly snapshots that are stored in S3 buckets. This can be used in the event of an accidental cluster deletion or for replication to a different cluster.

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, RTO/RPO and roles/responsibilities. Atlassian follows 'ISO22301 Business Continuity' as a guideline to their disaster recovery program.

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

F. Monitoring

The product operations and engineering teams continuously 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 PaaS (Platform as a Service) and monitoring platforms, which provide monitoring of application metrics, including AWS dependencies. The various monitoring tools include/cover:

- 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.

G. Incident Management

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

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

The standard principles of incident management consist of the following:

- Detection and recording — Atlassian has the appropriate tools in place to properly detect and record all incidents.
- Incident Classification for Resolution and Communication — Incidents are classified according to the level of severity. Incident Managers are a crucial part to exercising judgement 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 has the ability to resolve incidents immediately.
- Incident Handover — When incidents are escalated and run longer, incident handovers are coordinated.
- Closure and Post Incident Review — Clients/customers have the opportunity to provide feedback on the resolution of the incident. 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 Post Incident Review (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 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 particular root cause (Problem), they are reviewed for any other common incidents.

Atlassian uses four 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 ETA will take higher severity levels.
- Number of customers affected — This assessment is made on volume of customer tickets and % of traffic that is impaired or impacted.
- Customer/Internal service — Customer services such as support.atlassian.com.
- Is there any data loss — any potential data loss to customers increases severity.
- Security risks/breach — especially security breaches that 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.

H. Data Classification and Confidentiality of Information

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

- Information should be classified in terms of legal requirements, value, and criticality to Atlassian
- Information should be labeled to manage appropriate handling
- Manage all removable media with the same handling guidelines as below
- Media being disposed of should be securely deleted
- Media containing company information should be protected against unauthorized access, misuse, or corruption during transport

The following guidelines are used to classify data at Atlassian:

Rating	Description	Examples
Restricted	Information customers and staff have trusted to Atlassian's protection, which would be very damaging if released. Trust is the operative word.	● Customer Personally Identifiable Information (PII) ● Customer credit cards ● US Social Security numbers (customer or staff) ● Staff personal, bank, and salary details ● Sensitive company accounting data ● Decryption keys or passwords ● protecting information at this level ● Any other data Atlassian has a strong legal or moral requirement to protect
Public	Information freely available to the public.	● Any information available to the public ● Released source code ● Newsletters ● Information up on website
Internal	Information internal to Atlassian which 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 IP's ● Product announcements before the release date
Confidential	Information Atlassian holds which could cause damage to Atlassian	● Customer support issues logged on support site

Rating	Description	Examples
	or its customers if released. The default for any information customers has given us.	• Business plans and deals (including on extranet) • Information under an NDA • 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 Subservice Organizations Controls

Atlassian utilizes subservice organizations to perform certain functions as described in the description above. Rather than duplicate the control tests, controls at AWS and NTT are not included in the scope of this report. The affected criteria are included below along with the expected controls of AWS and NTT.

Criteria	Service Organization	Controls
CC6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	AWS	IT access above least privileged, including administrator access, is approved by appropriate personnel prior to access provisioning. IT access privileges are reviewed on a quarterly basis by appropriate personnel. User access to systems is revoked timely upon termination. Data is encrypted in transit in AWS.
CC6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	AWS	Physical access to the computer rooms, which house the entity's IT resources, servers, and related hardware, is restricted to authorized individuals through a badge access system or equivalent and monitored by video surveillance. Requests for physical access privileges require approval from an authorized individual. Electronic intrusion detection systems are installed and capable of detecting breaches into data center server locations. Documented procedures exist for the identification and escalation of potential security breaches. Visitors must be signed in by an authorized workforce member before gaining entry and must be escorted at all times.
	NTT	The Ashburn and Santa Clara Data Centers are remotely monitored by personnel from the Sterling and San Jose Data Centers, respectively. Data Center access is limited to authorized individuals through the use of access control cards. Additional security

Criteria	Service Organization	Controls
		mechanisms are implemented, as applicable. Customer assets, including hardware and network devices, are properly segregated from other customers using secured cabinets, cages, and suites. Access to the Data Centers is granted to NTT America associates based on their job responsibilities after the Associate Enrollment Form has been approved by NTT America management. Access to the Data Centers is granted to contractors based on their job responsibilities after the appropriate contractor and NTT America approvals are documented on the Contractor Enrollment Form. Quarterly user access reviews are performed on users that have access to the Hybrid Cloud, Console Pole Server, Ops Password and NetBackup/GMP systems. Changes are made to users' access based on the review, and approval of the review is maintained in the quarterly review log. NTT Security performs a review of data center access on at least a quarterly basis. Identified discrepancies between approval forms and access assigned are remediated.
CC8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	AWS NTT	Changes are authorized, tested, and approved prior to implementation.
A1.2: The entity authorizes, designs, develops or acquires, implements, operates, approves,	AWS NTT	Environmental protections have been installed including the following: • Cooling systems

Criteria	Service Organization	Controls
maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.		• Battery and generator backups • Smoke detection • Dry pipe sprinklers Environmental protection equipment receives maintenance on at least an annual basis.

Complementary User Entity Controls

Atlassian designed its controls with the assumption that certain controls will be the responsibility of its customers (or "user entities"). The following is a representative list of controls that are recommended to be in operation at user entities to complement the controls of the Atlassian Platform Systems. This is not a comprehensive list of all controls that should be employed by Atlassian's user entities.

- 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 8 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.
- Customers are responsible for managing access rights, including privileged access.
- 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.
- Customers are responsible for requesting, approving, and monitoring Atlassian's customer support access to their account.
- Customers are responsible for requesting their accounts to be removed.
- Customers are responsible for alerting Atlassian of incidents (related to Security, Availability, and Confidentiality) when they become aware of them.
- Customers are responsible for the security, including virus scans, and confidentiality of the data (e.g., media attachments) prior to the import or attachment and its ongoing monitoring after data has been uploaded.
- Customers are responsible for ensuring that their machines, devices, and network are secured.
- Customers are responsible for assessing and evaluating any potential impact add-ons may have on their instance.
- Bitbucket-specific -- Customers are responsible for performing periodic backups of their accounts and repositories for data beyond 7 days.
- Opsgenie-specific -- Customers are responsible for setting push notifications to active/on.
- Forge-specific -- App Developers are responsible for maintaining backups of their application code.

Section IV: Atlassian's Controls and Service Auditor's Tests of Controls and Results of Tests

Atlassian's Controls and Service Auditor's Tests of Controls and Results of Tests

Criteria and Controls

On the pages that follow, the applicable Trust Services Criteria and the controls to meet the criteria have been specified by and are the responsibility of Atlassian and the tests performed by EY and results are the responsibility of the service auditor.

Procedures for Assessing Completeness and Accuracy of Information Provided by the Entity (IPE)

For the controls requiring the use of IPE, including Electronic Audit Evidence (EAE) (e.g., controls requiring system-generated populations for sample-based testing), we perform a combination of the following procedures where possible based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used: (1) inspect the source of the IPE, (2) inspect the query, script, or parameters used to generate the IPE, (3) tie data between the IPE and the source, and/or (4) inspect the IPE for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintains its integrity. In addition to the above procedures, for controls requiring management's use of IPE in the execution of the controls (e.g., periodic reviews of user access listings), we inspect management's procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

Security, Availability, and Confidentiality Criteria Mapped to Atlassian's Controls, Service Auditor's Tests of Controls, and Results of Test

Entity Level Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
ELC-1	The organizational charts are reviewed by appropriate Atlassian management and updated semi-annually.	CC1.3	Inquired of the control owner and ascertained that the organizational charts were reviewed by appropriate Atlassian management and updated semi-annually, as appropriate.	No deviation noted.
			Inspected the organizational charts and ascertained that the appropriate Atlassian management reviewed and updated semi-annually, as appropriate.	No deviation noted.
ELC-2	Organizational charts are updated based on employee action notices and available to all Atlassian employees via Workday.	CC1.3	Inquired of the control owner and ascertained that organizational charts were updated based on employee action notices, and available to all Atlassian employees via Workday.	No deviation noted.
			Inspected the organization charts and ascertained that the organizational charts were updated based on employee action notices, and available to all Atlassian employees via Workday.	No deviation noted.
ELC-3	Policies are posted and available online, assigned a policy owner, and reviewed at least annually.	CC1.1 CC1.4 CC1.5 CC5.3 CC7.4	Inquired of the control owner and ascertained that policies were posted and available online, assigned a policy owner, and reviewed at least annually by the designated policy owner.	No deviation noted.
			Inspected the policies and ascertained that the policies were posted and available online, assigned a policy owner, and reviewed at least annually by the designated policy owner.	No deviation noted.

Entity Level Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
ELC-4	Audit Committee Charter defines roles, responsibilities, and key activities of the audit committee.	CC1.2 CC2.1 CC2.3 CC3.4	Inquired of the control owner and ascertained that Audit Committee Charter defined roles, responsibilities, and key activities of the audit committee.	No deviation noted.
			Inspected the Audit Committee Charter in the Atlassian's website and ascertained that roles, responsibilities, and key activities of the audit committee were defined.	No deviation noted.
ELC-5	The process of identifying and reviewing Board of Director Candidates is defined In Nominating and Governance Committee charter.	CC1.1 CC1.2 CC1.3 CC1.4	Inquired of the control owner and ascertained the process of identifying and reviewing Board of Director Candidates was defined in Nominating and Governance Committee charter.	No deviation noted.
			Inspected the Nominating and Governance committee charter and ascertained that the process of identifying and reviewing Board of Director Candidates was defined.	No deviation noted.
ELC-6	Qualifications for the Audit Committee's "Financial Expert" have been defined in the audit committee charter.	CC1.2 CC2.1 CC2.3 CC3.4	Inquired of the control owner and ascertained that the Audit Committee Charter defined the qualifications for the Audit Committee’s “Financial Expert”.	No deviation noted.
			Inspected the Audit Committee Charter in the Atlassian's website and ascertained that qualifications for the "Financial Expert" were defined.	No deviation noted.
ELC-7	Audit Committee meeting calendar and general meeting agenda are developed.	CC1.2 CC2.1 CC2.3	Inquired of the control owner and ascertained that Audit Committee meeting calendar and general meeting agendas were developed.	No deviation noted.

Entity Level Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
		CC3.4	Inspected the Audit Committee latest notice for the annual general meeting and ascertained that Audit Committee meeting calendar and general meeting agendas were developed.	No deviation 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.	CC1.1 CC1.2 CC1.3 CC1.4 CC1.5 CC2.1 CC2.2 CC2.3 CC3.1 CC4.1 CC4.2 CC5.2	Inquired of the control owner and ascertained that the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) reviewed committee charters and corporate governance which defined their roles, responsibilities, meeting frequency, participants, member qualifications on an annual basis.	No deviation noted.
			Inspected the current year's Board of Directors and subcommittee annual meeting minutes, and ascertained that committee charters and corporate governance, which defined their roles, responsibilities, meeting frequency, participants, and member qualifications, were discussed.	No deviation noted.
ELC-9	Financial statement risk assessment performed by Internal Audit and reviewed by Controller.	CC2.1 CC3.1	Inquired of the control owner and ascertained that on an annual basis, the Controller reviewed the financial statement risk assessments based on knowledge of the Company and against the assumptions used in the prior year.	No deviation noted.
			Inspected that most recent financial statement risk assessment and ascertained that the financial statement risk was reviewed by the Controller on an annual basis.	No deviation noted.

Entity Level Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
ELC-10	The Executive team sets strategic operational objectives annually.	CC1.1	Inquired of the control owner and ascertained the executive team had set Atlassian-level priorities annually.	No deviation noted.
			Inspected the Objectives and Key Results ("OKR") session minutes and ascertained that the executive team had set strategic operational objectives annually with each objective having an associated targeted result.	No deviation noted.
ELC-11	The signature authority matrix is maintained by Legal which establishes the signature authority for expenditures, contracts, capital acquisitions and write offs. Separately, the Corporate Controller established the cash disbursement.	CC3.1	Inquired of the control owner and ascertained the Spend Authority Limits (Signature Authority Matrix) was maintained by Legal, which establishes the signature authority for expenditures, contracts, capital acquisitions, and write offs. The Corporate Controller separately establishes the cash disbursement.	No deviation noted.
			Inspected the signature authority matrix and ascertained that legal approved and maintained the signature authority for expenditures, contracts, capital acquisitions, and write offs. Further ascertained that expenditure limits were reviewed annually during the Board of Directors meeting with the corporate controller establishing the cash disbursement.	No deviation noted.
ELC-12	Atlassian has established a Whistleblower hotline that is accessible to both external individuals and employees within the Company.	CC2.2 CC2.3	Inquired of the control owner and ascertained the Company had established a Whistleblower hotline that was accessible to both external individuals and employees within the Company.	No deviation noted.

Entity Level Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
			Inspected the Whistleblower hotline configuration and ascertained that the hotline was operating for external individuals and employees within the Company. Further inspected the notification alert and ascertained that all claims would notify to the General Counsel, Associate General Counsel, the Head of Internal Audit, and Audit Committee Chair.	No deviation noted.
ELC-13	The Head of Technical Accounting and Financial Reporting reviews the financials and footnote disclosures prepared by the member of Technical Accounting for reasonableness, internal consistency and confirms prior period balances of the final financial statements.	CC3.1	Inquired of the control owner and ascertained the Head of Technical Accounting and Financial Reporting reviewed the financials and footnote disclosures prepared by the member of Technical Accounting for reasonableness, internal consistency, and confirmed prior period balances of the final financial statements. A copy of the reviewed statements was then attached to an email to the CFO to evidence completion of review.	No deviation noted.
			Inspected the financials and footnote disclosures review and ascertained that the Head of Technical Accounting and Financial Reporting reviewed the financials and footnote disclosures prepared by a member of Technical Accounting for reasonableness and internal consistency and confirmed prior period balances in the financial statements.	No deviation noted.

Human Resource Controls

Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
HR-1	Hiring manager reviews and approves the job description prior to posting of job ads.	CC1.3	Inquired of the control owner and ascertained that hiring manager reviewed and approved the job description prior to posting of job ads.	No deviation noted.
			Inspected the configuration on Lever automation software and ascertained that it was configured to directly post job ads to the career page and respective job boards following approval from the respective hiring manager.	No deviation noted.
			Attempted to post a job ad to the career page without an approval and ascertained that the posting of job ads was rejected without appropriate approval.	No deviation noted.
			Inspected the hiring manager approvers for a sample of job ads posted and ascertained that the job descriptions for the job ads were reviewed and approved by the hiring manager prior to posting.	No deviation noted.
HR-2	Offer to external candidates are approved prior to hiring.	CC1.4 CC5.3	Inquired of the control owner and ascertained that offer to external candidates were approved prior to hiring. Further inquired and ascertained that for contractors who were hired outside of the standard hiring process, there was a confirmation of screening step in the onboarding process within Service Desk.	No deviation noted.
			Inspected a sample of job offers for new hires, interns, graduates, and contractors, and ascertained that job offers were reviewed and approved by a manager or confirmation of screening step in the onboarding process within Service Desk prior to hiring.	No deviation noted.

Human Resource Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
HR-3	Background checks are performed prior to their start dates. Results are reviewed against a results matrix and escalated to Legal and Head of HR Operations, if needed.	CC1.4	Inquired of the control owner and ascertained that background checks were performed prior to a new hire's start date. Results were reviewed against a results matrix and escalated to Legal and Head of HR Operations, if needed.	No deviation noted.
			Inspected the background check results for a sample of new employees and contractors and ascertained that background checks were performed prior to their start date. Further ascertained that results were reviewed against a results matrix and escalated to Legal and Head of HR Operations, if needed.	No deviation noted.
HR-4	Employees and contractors are required to sign CIIAs as part of the onboarding process.	CC1.5 CC2.2	Inquired of the control owner and ascertained that employees and contractors were required to sign CIIAs as part of the onboarding process.	No deviation noted.
			Inspected the signed CIIAs for a sample of new employees and contractors, and ascertained that employees and contractors were required to sign CIIAs as part of the onboarding process.	No deviation noted.
HR-5	Employees and contractors acknowledge the Code of Conduct annually.	CC1.1 CC1.5 CC2.2	Inquired of the control owner and ascertained that employees as well as contractors, acknowledged the Code of Conduct annually.	No deviation noted.
			Inspected the code of conduct acknowledgement for a sample of active employees and contractors, and ascertained that employees as well as contractors acknowledged the Code of Conduct annually.	No deviation noted.

Human Resource Controls

Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
HR-6	A weekly review is performed to determine that the CIIA (Confidential Information and Inventions Assignment) and background checks are completed for new employees prior to their start date.	CC2.2	Inquired of the control owner and ascertained that a weekly review was performed to determine that the CIIA (Confidential Information and Inventions Assignment) and that background checks were completed prior to their start date.	No deviation noted.
			Inspected the reviews for a sample of week and ascertained that a weekly review was performed to determine that new employees complete the CIIA (Confidential Information and Inventions Assignment), and background checks were completed prior to their start date.	No deviation noted.
HR-7	Performance appraisals are performed at least annually.	CC1.1 CC1.4 CC1.5 CC5.3	Inquired of the control owner and ascertained that performance appraisals were conducted at least annually.	No deviation noted.
			Inspected the performance appraisal results for a sample of employees and ascertained that performance appraisals were conducted at least annually.	No deviation noted.
HR-8	Training is provided to employees to support their continued development and growth.	CC1.4 CC1.5 CC5.3	Inquired of the control owner and ascertained that employees were provided with the necessary training and support to continue to learn and grow.	No deviation noted.
			Inspected the training homepage and ascertained that training and support were provided to employees through the training homepage and employees can continue to learn and grow.	No deviation noted.

Human Resource Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
HR-9	User awareness training is performed at least annually as part of the Atlassian Security Awareness program.	CC1.4 CC2.2	Inquired of the control owner and ascertained that user awareness training for malware risks was part of the security awareness program at Atlassian and performed at least on an annual basis.	No deviation noted.
			Inspected the user awareness training e-mail and security homepage and ascertained that security training, including passwords, phishing, and travel security, were provided to all employees as part of the security awareness program at Atlassian at least on an annual basis.	No deviation noted.

Customer Management and Communication Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
CMC-1	Significant changes made to the system are communicated to customers via the Atlassian customer facing website.	CC2.2 CC2.3 CC3.2	Inquired of the control owner and ascertained that significant changes made to the Systems were communicated to customers via the Atlassian customer facing website.	No deviation noted.
			Inspected the customer facing website and ascertained that significant changes made to the Systems were communicated.	No deviation 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.	CC2.2 CC2.3	Inquired of the control owner and ascertained that description of the Systems delineating the boundaries and describing relevant components were documented on the Atlassian intranet and the customer facing website.	No deviation noted.
			Inspected the customer-facing website and Atlassian intranet and ascertained that description of the Systems delineating the boundaries and describing relevant components were documented and posted in the Atlassian intranet and customer facing website.	No deviation noted.
CMC-3	Customer terms of service (ToS) are standardized and approved by legal. The terms of service (ToS) communicates Atlassian's commitments and the customer responsibilities. The ToS are published on the Atlassian customer facing website and any changes are communicated.	CC2.3	Inquired of the control owner and ascertained that customer terms of service ("ToS") were standardized and approved by legal. Further ascertained that the terms of service communicated Atlassian's commitments and customer responsibilities and were published on the Atlassian customer facing website. Any changes to the ToS were communicated timely.	No deviation noted.

Customer Management and Communication Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
			Inspected the Atlassian's ToS and ascertained that it was approved by legal and that it communicated Atlassian's commitments and customer responsibilities. Any changes to the ToS were communicated timely.	No deviation noted.
			Inspected the customer facing website and ascertained that Atlassian's ToS were published and that Atlassian's commitments and customer responsibilities were communicated to the customer prior to purchase of product, creation of user accounts.	No deviation noted.
CMC-4	Atlassian communicates changes to confidentiality commitments to its customers, vendors, and internal users through the Atlassian website, when applicable.	CC2.2 CC2.3	Inquired of the control owner and ascertained that Atlassian communicated changes to confidentiality commitments to its customers, vendors, and internal users through the Atlassian website, when applicable.	No deviation noted.
			Inspected the Atlassian's website and ascertained that communication on changes to confidentiality commitments to its customers, vendors, and internal users were posted when applicable.	No deviation noted.
CMC-5	Atlassian communicates its commitment to security as a top priority for its customers via Atlassian Trust Security page.	CC2.2 CC2.3 CC7.4 CC7.5	Inquired of the control owner and ascertained that Atlassian communicated its commitment to security as a top priority for its customers on the Atlassian Trust Security page.	No deviation noted.
			Inspected the Atlassian Trust Security Page and ascertained that Atlassian communicated its commitment to security as a top priority for its customers via Atlassian Trust Security page.	No deviation noted.

Customer Management and Communication Controls

Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
BBPL-1	Bitbucket Pipelines Removal of customer's Bitbucket repository data occurs within 7 days from the date of the termination of service.	CC6.5 CC6.7 C1.1 C1.2	Inquired of the control owner and ascertained that removal of customer's Bitbucket data from NetApp occurs within 7 days from the date of the termination of service and NetApp backup was removed after 7 days.	No deviation noted.
			Inspected the configuration in Bitbucket Cloud and ascertained that Bitbucket was configured to remove all customer's Bitbucket data from NetApp and NetApp's backup within 7 days.	No deviation noted.
			Inspected a sampled deleted customer and ascertained that the customer's data in NetApp and the NetApp's backup was removed within 7 days.	No deviation noted.
BBPL-2	Bitbucket Pipelines Bitbucket Pipelines customer data is deleted upon customer deletion request.	CC6.5 CC6.7 C1.1 C1.2	Inquired of the control owner and ascertained Bitbucket Pipelines' data was deleted upon receipt of a request for deletion.	No deviation noted.
			Inspected a sample of Bitbucket Pipelines customer data deletion request and ascertained that data was deleted timely.	No deviation noted.
OG-1	Opsgenie Opsgenie data is deleted within 30 days of receipt of a request for deletion.	CC6.5 CC6.7 C1.1 C1.2	Inquired of the control owner and ascertained Opsgenie data was deleted within 30 days of receipt of a request for deletion.	No deviation noted.
			Inspected the Opsgenie configuration and ascertained that customer data was automatically deleted within 30 days after the customer's request for deletion.	No deviation noted.
			Inspected a sampled request for deletion and ascertained that Opsgenie data was automatically deleted within 30 days of receipt based on the configuration.	No deviation noted.

Customer Management and Communication Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
PL-1	Jira, Confluence, JSM and Insight, Data Lake, Forge, and Compass Customer data is deleted from the Systems in a timely manner upon request or termination of the customer subscription.	CC6.5 CC6.7 C1.1 C1.2	Inquired of the control owner and ascertained that after the suspension of a client site or customer account (either due to customer-initiated non-renewal or the dunning process), customer data was deleted from Systems in a timely manner, as follows: • Jira Cloud, Confluence Cloud, JSM and Insight: Evaluators were removed within 15 days and non-evaluators were removed within 60 days. • Data Lake: Customer data was deleted upon suspension of customer account. • Forge: Customer data was deleted upon uninstallation of the Forge application within 15 days, and • Compass: Customer data was deleted upon deactivation of the instance in Compass.	No deviation noted.
			Jira Cloud, Confluence Cloud, JSM and Insight Inspected the account removal date for a sample of suspended customer accounts and ascertained that customer accounts were deleted per policy.	No deviation noted.

Customer Management and Communication Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
			Data Lake, Forge, Compass Inspected the data deletion configuration and ascertained that: • Customer data in Data Lake was deleted upon suspension of account, • Customer data in Forge was deleted upon uninstallation of the Forge application after 15 days, and • Customer data in Compass was deleted upon deactivation of the instance.	No deviation noted.
			Data Lake, Forge, Compass Inspected the account removal date for one sampled suspended customer account for Data Lake, Forge, and Compass, and ascertained that customer data were deleted upon suspension, deactivation, or uninstallation of the application per policy.	No deviation noted.
BBPL-3	Bitbucket and Bitbucket Pipelines Access to a customer repository is supported by a customer support request or internal incident.	CC6.1 CC6.2 CC6.3	Inquired of the control owner and ascertained that access to customer data by the Bitbucket support team was supported by a valid customer support request or internal incident.	No deviation noted.
			Inspected the Bitbucket configuration and ascertained that the Customer Consent Checker was configured to reject request to access customers' repositories without a valid open customer support ticket.	No deviation noted.
			Attempted to access customer data with a valid customer support ticket and ascertained that access was successfully granted.	No deviation noted.

Customer Management and Communication Controls

Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
			Attempted to access customer data without any valid customer support ticket and ascertained that access was denied.	No deviation noted.
			Attempted to access customer data with a valid and open customer support ticket unrelated to the attempted customer's repository, and ascertained that access was denied.	No deviation noted.
			Attempted to access customer data with a valid and closed customer support ticket, and ascertained that access was denied.	No deviation noted.
BBPL-4	Bitbucket and Bitbucket Pipelines Access to the Bitbucket Cloud Django Admin group is restricted to appropriate Atlassian team members.	CC6.1 CC6.2 CC6.3	Inquired of the control owner and ascertained that access to the Bitbucket Cloud Django Admin group was restricted to appropriate Atlassian team members.	No deviation noted.
			Inspected the Bitbucket Cloud Django Admin group and ascertained that access was restricted to appropriate Atlassian team members.	No deviation noted.
BBPL-5	Bitbucket and Bitbucket Pipelines Access to customer repositories by the Bitbucket internal support team is reviewed quarterly by the lead Support Engineer.	CC6.1 CC6.2 CC6.3	Inquired of the control owner and ascertained that access to customer repositories by the Bitbucket internal support team was reviewed quarterly by the lead Support Engineer.	No deviation noted.
			Inspected a sample of quarterly reviews of users with access to customer repositories and ascertained that access to customer's repositories by the Bitbucket internal support team was reviewed by the lead support engineer on a quarterly basis.	No deviation noted.

Customer Management and Communication Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
OG-2	Opsgenie Access to customer data by the Opsgenie Support team is supported by a valid and approved customer support request.	CC6.1 CC6.2 CC6.3	Inquired of the control owner and ascertained that access to customer data by the Opsgenie Support team was supported by a valid customer support request.	No deviation noted.
			Inspected the Opsgenie configuration and ascertained that upon a valid customer support request and customer consent, access to customer data was automatically provisioned to the Opsgenie support team via customer access link.	No deviation noted.
			Attempted to access customer data with a valid customer support request and ascertained that access was automatically granted to the Opsgenie Support team member.	No deviation noted.
			Observed a customer reject an access request from the Opsgenie Support team and ascertained that the Opsgenie Support team member was not able to access the customer data.	No deviation noted.
			Attempted to access customer data without a valid customer support request and ascertained that the Opsgenie Support team member's access was not granted.	No deviation noted.
PL-2	Jira, Confluence, JSM and Insight, Data Lake, Forge, and Compass Customer data is only accessed when supported by a valid	CC6.1 CC6.2 CC6.3	Inquired of the control owner and ascertained that access to customer data by the Customer Support and Success team was supported by a valid customer support request or an active incident that required access.	No deviation noted.

Customer Management and Communication Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
	customer support request or an active incident that requires access.		Jira Cloud, Confluence Cloud, JSM and Insight, Forge, and Compass Attempted to gain access to the Site Admin page of a customer using a valid open customer support request and ascertained that access was granted.	No deviation noted.
			Jira Cloud, Confluence Cloud, JSM and Insight, Forge, and Compass Attempted to gain access to the Site Admin page of a customer using the following tickets and ascertained that access was denied: • an invalid customer support ticket raised • a closed customer support ticket • an invalid open incident ticket, and • a closed incident ticket.	No deviation noted.
			Jira Cloud, Confluence Cloud, JSM and Insight, Forge, and Compass Inspected the logic in the Bitbucket repository and ascertained that accessed to customer data was automatically revoked within 48 hours upon provisioning.	No deviation noted.
			Jira Cloud, Confluence Cloud, JSM and Insight, Forge, and Compass Inspected a sampled user access review report and ascertained that the access to Governator was reviewed on a semi-annual basis.	No deviation noted.

Customer Management and Communication Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
			Jira Cloud, Confluence Cloud, JSM and Insight, Forge, and Compass Inspected the Jira tickets for a sample of customer support access to customer data and ascertained that the access was supported by a valid customer support request or an active incident that requires access.	No deviation noted.
DTL-1	Access to customer data is restricted to administrators and is only granted to developers on an as need and temporary basis to troubleshoot incidents.	CC6.1 CC6.2 CC6.3	Inquired of the control owner and ascertained that access to customer data was restricted to administrators and was only granted to developers on an as need and temporary basis to troubleshoot incidents.	No deviation noted.
			Inspected the Jira tickets for a sample of Customer Support and Success team access to customer data and ascertained that each access was supported by a valid customer support request and was restricted to administrators.	No deviation noted.
BBPL-6	Bitbucket and Bitbucket Pipelines Customer data is logically isolated.	CC6.1 CC6.6 CC6.7 C1.1	Inquired of the control owner and ascertained that customer data was logically isolated.	No deviation noted.
			Inspected the configuration in NetApp and ascertained that upon creation of a customer account, customer data was logically isolated. Additionally, inspected the configuration of the customer database and observed that unique constraints were enforced for each customer.	No deviation noted.
			Inspected a customer's data and ascertained that the customer's data is logically isolated.	No deviation noted.

Customer Management and Communication Controls

Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
OG-3	Opsgenie Opsgenie assigns unique identifiers to customer data upon creation.	CC6.1 CC6.6 CC6.7 C1.1	Inquired of the control owner and ascertained that Opsgenie assigned unique identifiers to customer data upon creation.	No deviation noted.
			Inspected the Opsgenie configuration and ascertained that all customers and users were configured to be provisioned with unique identifiers in Opsgenie.	No deviation noted.
			Inspected the creation of an account and ascertained that there was only one customer account with a unique identifier in the Opsgenie production database in both US and EU regions.	No deviation noted.
PL-3	Jira Cloud, Confluence Cloud, JSM and Insight, Forge, Compass, and Data Lake Customer data is logically segregated via unique identifiers which are attached for the lifetime of the data. The unique identifiers are used to determine which users can see which data.	CC6.1 CC6.6 CC6.7 C1.1	Inquired of the control owner and ascertained the following: • Customer data was logically separated in databases which each store the data for one tenant • A tenant was limited to one customer only • Each tenant was allocated a CloudID (a UUID), which was required to access the data.	No deviation noted.
			Jira Cloud, Confluence Cloud, JSM and Insight, Forge, Compass, and Data Lake Inspected the code used to create customer profiles and storage within a tenant and ascertained that a tenant was limited to the assigned customer and was not shared between multiple customers.	No deviation noted.

Customer Management and Communication Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
			Jira Cloud, Confluence Cloud, JSM and Insight, Forge, Compass, and Data Lake Inspected the creation of a customer tenant and ascertained that each tenant was allocated a CloudID (a UUID) which was required to access the data. Further ascertained that the same unique CloudID was assigned to each unique customer across the Atlassian Platform.	No deviation noted.
			Jira Cloud, Confluence Cloud, JSM and Insight, and Data Lake Inspected and obtained a listing of all customer records in the database and ascertained that customer data was logically separated in unique databases. Further ascertained that customers could only access their assigned database through their unique CloudID and credentials.	No deviation noted.
			Compass and Forge Inspected a sample Compass and Forge accounts and ascertained that there was only one customer account with a unique identifier in the Compass and Forge production databases.	No deviation noted.

Customer Management and Communication Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
CMC-6	Users may report bugs, defects, or availability, security, and confidentiality issues.	CC2.2 CC2.3 CC6.8 CC7.4 CC7.5	Inquired of the control owner and ascertained that customers and internal users contacted Atlassian to report issues on bugs, defects, availability, security, and confidentiality via social media, general website forms, https://support.atlassian.com, emails, https://trust.atlassian.com, public bug site, and Slack.	No deviation noted.
			Inspected the channels of reporting for issues and ascertained that customers and internal users were able to contact Atlassian to report issues on bugs, defects, availability, security, and confidentiality via social media, general website forms, https://support.atlassian.com, emails, https://trust.atlassian.com, public bug site, and Slack.	No deviation noted.
			Inspected a sample of issues reported by either internal or external users and ascertained that issues were followed up and resolved per incident management process.	No deviation noted.
BBPL-7	Bitbucket and Bitbucket Pipelines Active Bitbucket Cloud customers authenticate via Atlassian account where password configuration settings are managed.	CC6.1 CC6.2	Inquired of the control owner and ascertained that Bitbucket Cloud customers utilized Atlassian authentication and authorization methods.	No deviation noted.
			Inspected the configuration and ascertained that Bitbucket Cloud customers utilized Atlassian authentication and authorization methods.	No deviation noted.

Customer Management and Communication Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
			Observed the creation of a Bitbucket account in Bitbucket Cloud and ascertained that users utilized Atlassian authentication and authorization methods that met minimum password length of 8 characters and cannot reuse the last password used.	No deviation noted.
PL-4	Jira Cloud, Confluence Cloud, JSM and Insight, Forge, Compass, and Data Lake Unless an external identity provider is implemented by the customer, cloud customers must have a password that is, at a minimum, 8-characters in length.	CC6.1 CC6.2	Inquired of the control owner and ascertained that unless an external identity provider was implemented by the customer, cloud customers must have a password with a minimum length of 8-characters.	No deviation noted.
			Inspected the password configuration settings and ascertained that unless an external identity provider was implemented by the customer, cloud customers must have a password with a minimum length of 8-characters.	No deviation noted.

Enterprise Risk Management Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
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 their GRC tool.	CC1.2 CC3.1 CC3.2 CC3.4 CC4.1 CC4.2 CC5.1 CC5.2 CC5.3 CC9.1	Inquired of the control owner and ascertained that the Atlassian Risk and Compliance team evaluated the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Atlassian maintained a risk and controls matrix within their GRC tool (the Risk Management Jira project).	No deviation noted.
			Inspected the GRC Tool used by Atlassian and ascertained that the Atlassian Risk and Compliance team evaluated the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Further ascertained that Atlassian maintained a risk and controls matrix within their GRC tool (the Risk Management Jira project).	No deviation noted.
RM-2	Atlassian has defined an ERM process and conducts an enterprise risk assessment on an annual basis, which includes key product stakeholders.	CC3.1 CC3.2 CC4.1 CC4.2 CC5.1 CC5.2 CC5.3 CC9.1	Inquired of the control owner and ascertained that Atlassian had defined a risk management process and conducted an enterprise risk assessment on an annual basis, inclusive of key product stakeholders.	No deviation noted.
			Inspected the ERM assessment and ascertained that Atlassian had defined an ERM process, and the enterprise risk assessment was performed on an annual basis, which includes key product stakeholders. Additionally, a monthly meeting was held to discuss updates to the enterprise risk assessment and results.	No deviation noted.

Enterprise Risk Management Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
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 and a report. The results are included with the enterprise risk assessment which is communicated to the board and executive level managers annually.	CC2.1 CC2.3 CC3.1 CC3.2 CC3.3 CC5.1 CC5.2	Inquired of the control owner and ascertained that the fraud risk assessment was performed on an annual basis by the Head of Risk and Compliance. Further ascertained that this included a survey of employees susceptible to fraud and evaluation of external risks. The results were evaluated by the Head of Risk and Compliance and included in the enterprise risk assessment communicated to the board and executive level managers annually.	No deviation noted.
			Inspected the most recent enterprise risk assessment and ascertained that the enterprise risk assessment included a fraud risk assessment, which was performed and evaluated annually by the Head of Risk and Compliance.	No deviation noted.
			Inspected the most recent fraud and enterprise risk assessment and ascertained that the assessment was performed and evaluated annually by the Head of Risk and Compliance. Further ascertained that a cross-functional survey of employees in areas susceptible to fraud was conducted and combined with an evaluation of external risks, and the results were included with the enterprise risk assessment. Additionally, ascertained that the results were communicated to the board and executive level managers as part of the annual meeting held.	No deviation noted.

Enterprise Risk Management Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
RM-4	Internal audits are performed, results are communicated to management and Audit Committee, and corrective actions are monitored.	CC2.1 CC3.1 CC3.2 CC4.1 CC4.2 CC5.1 CC5.2 CC5.3	Inquired of the Internal Audit and ascertained that internal audits were performed relating to SOX, ISO, SOC, and other operational audits. Further ascertained that results were communicated to management and Audit Committee, and corrective actions were monitored.	No deviation noted.
			Inspected the GRC tool (the Risk Management Jira project) and Jira ticket and ascertained that internal audits were performed relating to SOX, ISO, SOC, and other operational audits. Further ascertained that results were communicated to management and Audit Committee, and corrective actions were monitored.	No deviation noted.

Change Management Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
CHG-1	Bitbucket and Opsgenie Peer review and passed green build testing is required prior to production deployment.	CC2.1 CC6.8 CC8.1	Inquired of the control owner and ascertained that changes were documented through pull requests, and peer review and passed green build testing were required prior to merging the code to the production branch.	No deviation noted.
			Inspected the Bitbucket configuration and ascertained that the Bitbucket and Opsgenie repositories did not allow changes to deploy or run on the platform unless they had been peer reviewed. Further inspected Deployment Bamboo and determined that changes required code to pass green build testing prior to merging.	No deviation noted.
			Attempted to merge a pull request with a peer review and green build testing and ascertained that it was successfully merged to the production branch.	No deviation noted.
			Attempted to merge a pull request without peer review and green build testing and ascertained that the code was not merged to the production branch.	No deviation noted.
			Inspected a sample of merged pull requests and ascertained that documented peer review and green build testing was required prior to merging the code to production branch.	No deviation noted.
MICROS-1	Jira, Confluence, JSM and Insight, Forge, Compass, and Data Lake The Micros platform will not allow code artifacts to deploy or	CC2.1 CC6.8 CC8.1	Inquired of the control owner and ascertained that changes were documented through pull requests, and peer review and passed green build testing was required prior to merging the code to the master branch.	No deviation noted.

Change Management Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
	run on the platform unless they have been peer reviewed and have passed green build testing.		Inspected the Bitbucket configuration and ascertained that changes were documented through pull requests, and that the Micros repositories would not allow changes to deploy or run on the platform unless they have been peer reviewed and have passed green build testing.	Jira, Confluence, JSM and Insight, and Data Lake No deviation noted. Compass and Forge Deviation noted. One (1) code repository for Compass and two (2) code repositories for Forge had a bot account with write access to override the configuration settings in Bitbucket.
			Inspected a sample of merged pull requests and ascertained that documented peer review and green build testing was required prior to merging the code to master branch.	No deviation noted.
Management Response: For Compass and Forge, bot accounts require write access to the repositories to facilitate the CI/CD process. Access to the accounts are tightly restricted based on least privilege. Atlassian has reviewed all changes made by the bot accounts and confirmed that these were all valid and authorized (PL-4).				
PL-5	Compass, Forge Bot account changes are reviewed periodically for	CC2.1 CC6.8 CC8.1	Inquired with the control owner and ascertained that Bot account changes were reviewed periodically for appropriateness and authorization.	No deviation noted.

Change Management Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
	appropriateness and authorization.		Inspected the Bot accounts review for Forge and Compass and ascertained that the Bot accounts changes were reviewed periodically for appropriateness and authorization.	No deviation noted.
MICROS-2	Micros will only pull deployment artifacts from the restricted namespace. Only Deployment Bamboo has the credentials to push to the restricted namespace	CC2.1 CC6.8 CC8.1	Inquired of the control owner and ascertained that artifacts with peer review and passed green build testing were deployed from a restricted namespace by Deployment Bamboo bot account.	No deviation noted.
			Inspected the list of accounts with ability to commit changes to Docker and ascertained that only Deployment Bamboo was assigned to push changes to Docker.	No deviation noted.
			Attempted to push a change to the restricted Docker namespace using an end user account and ascertained that the deployed change was denied.	No deviation noted.
CHG-2	Bitbucket and Opsgenie Bitbucket does not allow a pull request to be approved by the same user who requests it.	CC2.1 CC6.8 CC8.1	Inquired of the control owner and ascertained that Bitbucket did not allow a pull request to be approved by the same user who requested it.	No deviation noted.
			Inspected the Bitbucket configuration and ascertained that Bitbucket did not allow a pull request to be approved by the same user who requested it.	No deviation noted.
			Attempted to merge a pull request where the requester is the same as the approver and ascertained that the pull request was not merged.	No deviation noted.

Change Management Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
			Attempted to merge a pull request where the requester is different from the approver and ascertained that the pull request was merged.	No deviation noted.
			Inspected a sample of merged pull requests and ascertained that the peer review requester was not the same as the approver.	No deviation noted.
BBPL-8	Bitbucket Merging code to the production branch of Bitbucket Cloud requires a peer reviewed pull request.	CC2.1 CC6.8 CC8.1	Inquired of the control owner and ascertained that merging a code directly to the production branch without going through staging branch was not allowed.	No deviation noted.
			Inspected the Bitbucket Cloud configuration and ascertained that the Bitbucket platform repositories would not allow code artifacts to be merged to the production branch without a peer reviewed pull request.	No deviation noted.
			Inspected a sample of merged pull requests and ascertained that a peer reviewed pull request was required prior to merging the code to production branch.	No deviation noted.
CHG-3	Bitbucket, Jira, Confluence, JSM and Insight, Forge, Data Lake, and Compass Deployment Bamboo will not allow code to be deployed unless it has passed green build testing. A green build (successful build) occurs when all the automated tests as defined within the Deployment Bamboo build plan have	CC2.1 CC6.8 CC8.1	Inquired of the control owner and ascertained that Deployment Bamboo did not allow code to be deployed unless it had passed green build testing.	No deviation noted.
			Attempted to deploy a green build code and ascertained that Deployment Bamboo allowed the code to be deployed.	No deviation noted.
			Attempted to deploy a red build code and ascertained that it did not allow the code to be deployed unless it has passed green build testing.	No deviation noted.

Change Management Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
	successfully completed. A red build occurs if any tests defined within the Bamboo build plan fail.		Inspected a sample of deployed builds and ascertained that green build testing was required prior to deploying to production.	No deviation noted.
CHG-4	Bitbucket, Jira, Confluence, JSM and Insight, Forge, Data Lake, and Compass Deployment Bamboo performs a check to validate that the SOX setting on Bitbucket are compliant to following: • Requires >1 approver • Unapproved automatically on new changes • Changes without a pull request. If the settings are not compliant, the code is rejected.	CC2.1 CC6.8 CC8.1	Inquired of the control owner and ascertained that Deployment Bamboo performed a check to validate that the SOX settings on Bitbucket were compliant to following: • Requires >1 approver • Unapproved automatically on new changes • Changes without a pull request. If the settings were not compliant, the code is rejected.	No deviation noted.
			Inspected the API configuration in Deployment Bamboo and ascertained that a check was performed to validate that the SOX settings on Bitbucket were compliant to the following: • Requires >1 approver • Unapproved automatically on new changes • Changes without a pull request. If the settings were not compliant, the code is rejected.	No deviation noted.
			Attempted to deploy a change that was compliant and ascertained that the code was successfully deployed upon the validation check in Deployment Bamboo.	No deviation noted.

Change Management Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
			Attempted to deploy a change that was not compliant and ascertained that the code was rejected for deployment upon the validation check in Deployment Bamboo.	No deviation noted.
BBPL-9	Bitbucket Operating system, database, Puppet, deployment script, and emergency changes follow the same process as the application changes.	CC2.1 CC6.8 CC8.1	Inquired of the control owner and ascertained that operating system, database, Puppet, deployment script, and emergency changes followed the same process as the application changes.	No deviation noted.
			Inspected the Bitbucket configuration and ascertained that the same application change settings were configured for operating system, database, Puppet, deployment script, and emergency changes.	No deviation noted.
			Inspected a sample of merged pull requests and ascertained that the changes follow the same process as the application changes (peer review and green build testing).	No deviation noted.
BBPL-10	Bitbucket Puppet is used to manage the configuration of the databases and servers used in production.	CC2.1 CC6.8 CC8.1	Inquired of the control owner and ascertained that Puppet was used to manage the configuration of the databases and servers used in production.	No deviation noted.
			Inspected the Puppet configuration and ascertained that Puppet is used to manage the configuration of the databases and servers used in production.	No deviation noted.
			Attempted to merge a pull request and ascertained that changes were required to pass tests and be reviewed prior to being applied.	No deviation noted.

Change Management Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
			Inspected the Puppet configuration and ascertained that it enforces the server configuration every 30 minutes.	No deviation noted.
			Inspected a sample of merged pull requests and ascertained that Puppet policy files required peer review and changes were required to pass tests and be reviewed prior to being applied.	No deviation noted.
OG-4	Opsgenie Only artifacts that have a valid signature from the build software can be released to the production environment.	CC2.1 CC6.8 CC8.1	Inquired of the control owner and ascertained that only artifacts with a valid signature from the build software could be released to the production environment.	No deviation noted.
			Inspected the Bitbucket and AWS configuration and ascertained that artifacts without a valid GPG tag or "signature" could not be released to the production environment.	No deviation noted.
			Attempted to release an artifact to production without a valid GPG tag or "signature" and ascertained that the change could not be released to the production environment.	No deviation noted.
			Attempted to release an artifact to production with a valid GPG tag or "signature" and ascertained that the change could was released to the production environment.	No deviation noted.
OG-5	Opsgenie No users have access to directly release a build or modify any build artifacts into S3 or deploy a change directly into the	CC2.1 CC6.8 CC8.1	Inquired of the control owner and ascertained that 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.	No deviation noted.

Change Management Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
	Opsgenie production environment.		Inspected the S3 configuration and ascertained that 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.	No deviation noted.
			Attempted to directly release a build or modify a build artifact in S3 or deploy a change directly into the Opsgenie production environment and ascertained that the change was rejected.	No deviation noted.
CHG-5	A Jira ticket is automatically generated if a change to the enforcement of peer review occurs.	CC2.1 CC6.8 CC8.1	Inquired of the control owner and ascertained that a Jira ticket was automatically generated if a change to the enforcement of peer review occurs.	No deviation noted.
			Inspected the configuration and ascertained that a Jira ticket was automatically generated if a change to the enforcement of peer review occurs.	No deviation noted.
CHG-6	For Bitbucket, Jira, Confluence, JSM and Insight, Forge, Data Lake, 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.	CC2.1 CC6.8 CC8.1	Inquired of the control owner and ascertained that Tokenator performed a check to validate that the Compliance settings on Bitbucket were enabled prior to building the code.	No deviation noted.
			Inspected the configuration and ascertained that Tokenator performed a check to validate that the Compliance settings on Bitbucket repositories' master/production branches were enabled prior to building the code.	No deviation noted.
			Attempted to deploy a change that was not compliant and ascertained that the code was rejected for deployment upon the validation check.	No deviation noted.

Change Management Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
			Attempted to deploy a change that was compliant and ascertained that the code was successfully deployed upon the validation check in Deployment Bamboo.	No deviation noted.
CHG-7	Bitbucket, Jira, Confluence, JSM and Insight, Forge, Data Lake, Compass All changes to the master branch of Deployment Bamboo in-scope repositories require a peer reviewed pull request.	CC2.1 CC6.8 CC8.1	Inquired of the control owner and ascertained that the master branch of Deployment Bamboo in-scope repositories required a peer reviewed pull request.	No deviation noted.
			Inspected the configurations of Deployment Bamboo in-scope repositories and ascertained that a change to the master branch of such repositories required a peer reviewed pull request.	No deviation noted.
			Inspected a sample of pull requests made to the master branch of Deployment Bamboo in-scope repositories and ascertained that peer reviews were performed for the sampled pull requests.	No deviation noted.
CHG-8	Bitbucket, Jira, Confluence, JSM and Insight, Forge, Data Lake, Compass Changes to the Deployment Bamboo product are tested by the Build Engineering team prior to upgrading internal Deployment Bamboo servers.	CC2.1 CC6.8 CC8.1	Inquired with the control owner and ascertained that changes to the Bamboo product were tested by the Build Engineering team prior to upgrading internal Deployment Bamboo servers.	No deviation noted.
			Inspected configurations of automatic tests and ascertained that automated tests run each time a newer release of Deployment Bamboo was deployed.	No deviation noted.
			Inspected a sample of changes to the Deployment Bamboo product and ascertained that testing was performed prior to upgrading the internal Deployment Bamboo servers.	No deviation noted.

Change Management Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
CHG-9	Bitbucket, Bitbucket Pipelines, Jira, Confluence, JSM and Insight, Forge, Data Lake, Compass Changes to Bitbucket Pipelines must be peer reviewed prior to production deployment.	CC2.1 CC6.8 CC8.1	Inquired with the control owner and ascertained that changes to Bitbucket Pipelines were peer reviewed prior to production deployment.	No deviation noted.
			Inspected the Bitbucket configuration and ascertained that the Bitbucket Pipelines repositories would not allow changes to deploy unless they had been peer reviewed.	No deviation noted.
			Inspected a sample of merged pull requests and determined that documented peer review was required prior to deployment to production.	No deviation noted.
CHG-10	Bitbucket, Bitbucket Pipelines, Jira, Confluence, JSM and Insight, Forge, Data Lake, Compass Bitbucket Pipelines will not allow code to be deployed unless it has passed green build testing.	CC2.1 CC6.8 CC8.1	Inquired of the control owner and ascertained that Bitbucket Pipelines does not allow code to be deployed unless it has passed green build testing.	No deviation noted.
			Inspected the configuration and ascertained that Bitbucket Pipelines does not allow code to be deployed unless it has passed green build testing.	No deviation noted.
			Attempted to deploy a red build code and ascertained that it did not allow the code to be deployed unless it has passed green build testing.	No deviation noted.
			Attempted to deploy a green build code and ascertained that Bamboo allowed the code to be deployed.	No deviation noted.
			Inspected a sample of builds within Bitbucket Pipelines and ascertained that a passed green build testing was required prior to deployment.	No deviation noted.

Change Management Controls

Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
CHG-11	Bitbucket, Bitbucket Pipelines, Jira, Confluence, JSM and Insight, Forge, Data Lake, Compass Write access to production software artifacts in Artifactory is limited to the Build Engineering team, the automated build system, and the Micros server.	CC2.1 CC6.1 CC6.2 CC6.3 CC6.8 CC8.1	Inquired of the control owner and ascertained that write access to production software artifacts was limited to the Build Engineering team and the automated build system.	No deviation noted.
			Inspected the write access to Artifactory and ascertained that write access to production software artifacts was limited to the Build Engineering team, the automated build system, and the Micros server.	No deviation noted.
MGRT-1	Bitbucket and Bitbucket Pipelines Procedures exist to monitor completeness and accuracy of customer data migrated from NTT data center in Ashburn (ASH2) to the Micros platform hosted in AWS.	A1.1	Inquired of the control owner and ascertained that procedures exist to monitor completeness and accuracy of customer data migrated from the NTT data center in Ashburn (ASH2) to the Micros platform hosted in AWS.	No deviation noted.
			Inspected the Bitbucket data migration plan and ascertained that there were procedures in place to monitor completeness and accuracy of the customer data migration from the NTT data center in Ashburn (ASH2) to the Micros platform hosted in AWS.	No deviation noted.
			Inspected the Bitbucket data migration testing performed by management and ascertained that a sample of users were tested to ensure that data was completely and accurately migrated from the NTT data center in Ashburn (ASH2) to the Micros platform hosted in AWS.	No deviation noted.

Access Management Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
IAM-1	Two-factor authentication is required when logging into VPN (Remote Access Service) from any IP address.	CC6.1 CC6.2 CC6.6	Inquired of the control owner and ascertained that two-factor authentication was required when logging into VPN (Remote Access Service) from any IP address.	No deviation noted.
			Inspected the network configuration used on internal network endpoints and ascertained that two-factor authentication was required when logging into VPN (Remote Access Service) from any IP address.	No deviation noted.
			Attempted to access the VPN with and without the two-factor authentication and ascertained that two-factor authentication was required.	No deviation noted.
IAM-2	Two-factor authentication is required when launching an application from the single sign on system (Idaptive).	CC6.1 CC6.2 CC6.6	Inquired of the control owner and ascertained that Duo was integrated to Idaptive to require two-factor authentication and Duo also extended two-factor protection to applications launched from a Idaptive browser session. Further ascertained that Duo two-factor authentication was required when logging in from any IP that was not whitelisted within the "exempt IP" settings in Idaptive.	No deviation noted.
			Inspected the configuration between Idaptive and Duo and ascertained that two-factor authentication was enforced for all login attempts for non-Atlassian office networks or from any IP that was not whitelisted within the "exempt IP" settings in Idaptive. Further inspected all IP addresses listed as exempt from Duo two-factor authentication and determined that these belong to Atlassian Office networks and verified that these were	No deviation noted.

Access Management Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
			appropriate to be exempt from Duo two-factor authentication.	
			Attempted to login to Idaptive, any application from a Idaptive browser session, and from an IP not whitelisted in Idaptive, and ascertained that two-factor authentication was required using Duo.	No deviation noted.
IAM-3	Access to the Atlassian internal network and internal tools is restricted to authorized users via logical access measures: • Each Atlassian user must have an active Directory account. • Each Atlassian user must be members of the appropriate LDAP group.	CC6.1 CC6.2 CC6.3 CC6.6	Inquired of the control owner and ascertained that access to the Atlassian internal network and internal tools were restricted to authorized users via logical access measures: • Each Atlassian user must have an active Directory account. • Each Atlassian user must be members of the appropriate LDAP group.	No deviation noted.
			Inspected the configuration and ascertained that access to the Atlassian internal network and internal tools were restricted to authorized users via logical access measures: • Each Atlassian user must have an active Directory account. • Each Atlassian user must be members of the appropriate LDAP group.	No deviation noted.
			Observed an Atlassian user getting access to the internal network and internal tools, and ascertained that access was prohibited as the user was not assigned to the appropriate LDAP group or an active Directory account.	No deviation noted.

Access Management Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
			Observed an Atlassian user getting access to the internal network and internal tools and ascertained that the user had an active Directory account and a member of an appropriate LDAP group.	No deviation noted.
IAM-4	Active Directory group membership is automatically assigned based on the user's department and team.	CC6.1 CC6.3	Inquired of the control owner and ascertained Active Directory group membership was automatically assigned based on the user's department and team.	No deviation noted.
			Inspected the configuration and ascertained that Active Directory group membership was automatically assigned based on the user's department and team in Workday.	No deviation noted.
			Inspected a sample user's Active Directory group membership and ascertained that it was based on the user's department and team in Workday.	No deviation noted.
IAM-5	Active Directory enforces password settings in line with the Atlassian Password Standard. Idaptive Single Sign On allows users to have a single point of authentication to access multiple applications. Passwords settings for Idaptive are enforced by Active Directory (AD) via the AD connector for Idaptive.	CC6.1 CC6.2	Inquired of the control owner and ascertained that Idaptive single sign-on allowed users to have a single point of authentication to access multiple applications and enforced minimum password length configured in Active Directory, which was in line with the Atlassian Password Standard.	No deviation noted.
			Observed a user login to Idaptive and ascertained that single sign-on allowed users to have a single point of authentication to access multiple applications, and minimum password length was configured in Active Directory and enforced by Idaptive which was in line with the Atlassian Password Standard.	No deviation noted.

Access Management Controls				
Control #	**Controls Specified by Atlassian**	**Criteria**	**Tests of Controls**	**Results of Test**
MICROS-3	Bitbucket, Bitbucket Pipelines, Jira, Confluence, JSM and Insight, Forge, Data Lake, Compass Direct access to the Micros Platform via JumpBox requires a valid SSH key and two factor authentication.	CC6.1 CC6.2 CC6.3 CC6.6	Inquired of the control owner and ascertained that direct access to the Micros Platform via JumpBox required a valid SSH key and two-factor authentication.	No deviation noted.
			Inspected the network configuration and ascertained that direct access to the Micros Platform via JumpBox required a valid SSH key and two-factor authentication.	No deviation noted.
			Attempted access to the Micros Platform via JumpBox with and without a valid SSH key and ascertained that a valid SSH key and two-factor authentication was required.	No deviation noted.
MICROS-4	Bitbucket, Bitbucket Pipelines, Jira, Confluence, JSM and Insight, Forge, Data Lake, Compass Privileged access of Atlassian users to EC2 production environment is restricted to authorized and appropriate users only.	CC6.1 CC6.2 CC6.3 C1.1	Inquired of the control owner and ascertained privileged access of Atlassian users to EC2 production environment was restricted to authorized and appropriate users only.	No deviation noted.
			Inspected the complete list of users with privileged access to EC2 production environment and ascertained that access was restricted to authorized and appropriate users only.	No deviation noted.
MICROS-5	Bitbucket, Bitbucket Pipelines, Jira, Confluence, JSM and Insight, Forge, Data Lake, Compass Access to the AWS production environment, RDS databases, and supporting tools is provisioned based on appropriate authorization by the service owner or delegate.	CC6.2 CC6.3	Inquired of the control owner and ascertained that access to the AWS production environment, RDS databases, and supporting tools was provisioned based on the appropriate authorization by the service owner or delegate.	No deviation noted.
			Inspected the supporting evidence for a sample of users granted access to the AWS production environment, RDS databases, and supporting tools, and ascertained that the	No deviation noted.

Access Management Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
			access was approved appropriately prior to being provisioned.	
BBPL-11	Bitbucket (11/1/2020 to 8/26/2021) Direct access to CentOS servers and PostgreSQL requires a valid SSH key.	CC6.1 CC6.2 CC6.3 CC6.6	Inquired of the control owner and ascertained that direct access to CentOS servers required a valid SSH key.	No deviation noted.
			Inspected the configuration settings in CentOS and ascertained that direct access to CentOS servers required a valid SSH key.	No deviation noted.
			Attempted to login to CentOS with a valid SSH key, and ascertained that access was allowed to CentOS servers.	No deviation noted.
			Attempted to login to CentOS without an SSH key and ascertained that direct access to CentOS servers required a valid SSH key.	No deviation noted.
BBPL-12	Bitbucket (11/1/2020 to 8/26/2021) Direct access to PostgreSQL requires a unique username and password.	CC6.1 CC6.2 CC6.3	Inquired of the control owner and ascertained that direct access to PostgreSQL required a unique username and password.	No deviation noted.
			Inspected the list of SSH keys from the Bitbucket Cloud server and ascertained that each SSH key was associated to a unique UserID, and direct access to PostgreSQL required a unique username and password.	No deviation noted.
			Inspected the list of usernames from PostgreSQL and ascertained that each username was unique.	No deviation noted.

Access Management Controls

Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
IAM-6	An automatic alert is triggered to the Risk and Compliance Manager and HR for any role change between the following groups: Engineering, Customer Support & Success (CSS), or Finance group. Appropriateness of access is reviewed and approved.	CC6.1 CC6.2 CC6.3	Inquired of the control owner and ascertained that an automatic alert was triggered to the Risk and Compliance Manager and HR for any role change between the following groups: Engineering, Customer Support and Success ("CSS"), or Finance group. Further ascertained that appropriateness of access was reviewed and approved.	No deviation noted.
			Inspected a sample of role changes between the Engineering, Customer Support and Success ("CSS"), or Finance group, and ascertained that an automatic alert was triggered to the Risk and Compliance Manager and HR, and appropriateness of access was reviewed and approved.	Deviation noted. For two (2) of the three (3) sampled users' who transferred between security divisions their access was not reviewed and approved timely.
Management Response: Atlassian has retrospectively reviewed the excluded accounts and deemed that the accounts were appropriate. Atlassian has updated procedures to ensure completeness of future reviews. Additionally, user access reviews performed at the application level had no deviations noted and served as compensating controls (MICROS-6, BBPL-12, BBPL-13, OG-05, PL-05).				
IAM-7	Active directory accounts and network access are automatically disabled within 8 hours from the time an employee is marked as terminated in the HR system.	CC6.1 CC6.2	Inquired the control owner and ascertained that within up to 8 hours of a user account being marked as inactive in Workday, user accounts were disabled in Idaptive and Active Directory, including being removed from associated Active Directory groups.	No deviation noted.

Access Management Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
			Inspected the job configured to run between Workday and Idaptive and ascertained that the Active Directory account of terminated users were automatically suspended within up to eight (8) hours upon termination.	No deviation noted.
			Inspected the access removal date in Active Directory for a sampled terminated user and ascertained that access was removed timely for the sampled user.	No deviation noted.
			Inspected the SignalFX monitoring and history log of the Idaptive job and ascertained that failure in the job was investigated and resolved timely.	No deviation noted.
IAM-8	The HR system does not allow terminations to be backdated.	CC6.1 CC6.2	Inquired of the control owner and ascertained that HR system does not allow terminations to be backdated.	No deviation noted.
			Inspected the Workday configuration and ascertained that the HR system does not allow terminations to be backdated.	No deviation noted.
			Attempted to backdate an employee in Workday and ascertained that the HR system did not allow terminations to be backdated.	No deviation noted.
IAM-9	On a semi-annual basis, the Build Engineering Development Team Lead performs a review of privileged user access for Deployment Bamboo.	CC2.1 CC6.1 CC6.2 CC6.3 CC8.1	Inquired of the control owner and ascertained that the Build Engineering Development Team Lead performed a review of privileged user access for Deployment Bamboo semi-annually.	No deviation noted.
			Inspected the documentation of a sampled user access review and ascertained that the Build Engineering Development Team Lead performed a review of privileged user access for Deployment Bamboo semi-annually.	No deviation noted.

Access Management Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
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.	CC6.1 CC6.2 CC6.3	Inquired of the control owner and ascertained that Active Directory and Idaptive user access reviews for privileged users were performed on a semi-annual basis.	No deviation noted.
			Inspected the report for a sample of user access review and ascertained that access reviews were performed on a semi-annual basis. Further ascertained that discrepancies identified in the access review were investigated and resolved.	Deviation noted. The review selected for testing was not complete and accurate as it excluded two (2) accounts with privileged access to Idaptive.
Management Response: Atlassian has reviewed the accounts of the users who transferred, made necessary access changes, and has updated procedures to help ensure completeness of future reviews. Additionally, user access reviews performed at the application level had no deviations noted and served as compensating controls (MICROS-6, BBPL-13, BBPL-14, OG-6, PL-6).				
MICROS-6	Bitbucket, Bitbucket Pipelines, Jira, Confluence, JSM and Insight, Forge, Data Lake, 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.	CC6.1 CC6.2 CC6.3	Inquired of the control owner and ascertained that the 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 deviation noted.
			Inspected a sampled user access review report and ascertained that the 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 deviation noted.

Access Management Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
BBPL-13	Bitbucket Privileged access to software the Bitbucket Cloud team uses to administer the service is reviewed semi-annually.	CC6.1 CC6.2 CC6.3	Inquired of the control owner and ascertained that privileged access to software the Bitbucket Cloud team used to administer the service was reviewed semi-annually.	No deviation noted.
			Inspected the semi-annual user access review report around privileged access to Bitbucket Cloud software, including supporting applications, that was performed, and ascertained that privileged access to software the Bitbucket Cloud team used to administer the service was reviewed semi-annually.	No deviation noted.
OG-6	Opsgenie The Opsgenie user access review is performed on a semi-annual basis; including shared, generic, and bot accounts.	CC6.1 CC6.2 CC6.3	Inquired of the control owner and ascertained that the privileged access review, including shared, generic, and bot account, was performed semi-annually.	No deviation noted.
			Inspected a sampled user access review report over privileged access to Opsgenie and supporting systems and ascertained that the review was performed on a semi-annual basis and that privileged user access including shared, generic, and bot accounts in Opsgenie were reviewed.	No deviation noted.
PL-6	Forge, Data Lake, JSM and Insight User access reviews are performed on a semi-annual basis and issues identified are remediated in a timely manner.	CC6.1 CC6.2 CC6.3	Inquired of the control owner and ascertained a user access review over the Forge, Data Lake, and Jira Service Management and Insight production environment was performed semi-annually, and issues identified were remediated in a timely manner.	No deviation noted
			Inspected the documentation of a sampled user access review and ascertained that a review of privileged user access for Forge,	No deviation noted

Access Management Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
			Data Lake, and Jira Service Management and Insight were performed semi-annually. Issues identified were remediated in a timely manner.	
BBPL-14	Bitbucket and Bitbucket Pipelines Access to AWS Glacier is restricted to members of the Bitbucket DevOPs and SRE team.	CC6.1 CC6.2 CC6.3 A1.2	Inquired of the control owner and ascertained that access to AWS Glacier was restricted to members of the Bitbucket DevOPs and SRE team.	No deviation noted.
			Inspected the list of users with access to AWS Glacier and ascertained that access to AWS Glacier was restricted to members of the Bitbucket DevOPs and SRE team.	No deviation noted.
OG-7	Opsgenie Privileged access to AWS services within the AWS console is restricted to authorized and appropriate users.	CC6.1 CC6.2 CC6.3	Inquired of the control owner and ascertained that privileged access to AWS within the AWS Console was restricted to authorized and appropriate users.	No deviation noted.
			Inspected the complete list of users with privileged access to the AWS production console and ascertained that access was restricted to authorized and appropriate user.	No deviation noted.
BBPL-15	Bitbucket (11/1/2020 to 8/26/2021) Direct access to PostgreSQL is approved prior to granting access.	CC6.1 CC6.2 CC6.3 CC6.6	Inquired of the control owner and ascertained that direct access to PostgreSQL was approved prior to granting access.	No deviation noted.
			Inspected the ticket for a sample of new users who were granted access to PostgreSQL via SSH keys and ascertained that direct access to PostgreSQL was approved prior to granting access.	No deviation noted.

Access Management Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
BBPL-16	Bitbucket CentOS SSH keys are rotated annually.	CC6.1 CC6.2	Inquired of the control owner and ascertained that CentOS SSH keys were rotated annually.	No deviation noted.
			Inspected the configuration in Bitbucket Cloud server and ascertained that CentOS SSH keys were configured to expire and rotate annually.	No deviation noted.
			Inspected a sample of users with SSH keys and ascertained that their CentOS SSH keys were rotated annually.	No deviation noted.
BBPL-17	Bitbucket Pipelines Access to Bitbucket Pipelines systems is provisioned based on appropriate authorization by the service owner or delegate.	CC6.2 CC6.3	Inquired of the control owner and ascertained that access to Bitbucket Pipelines systems is provisioned based on appropriate authorization by the service owner or delegate.	No deviation noted.
			Inspected the provisioning log for a sample of user granted to Bitbucket Pipelines access and ascertained that the access was provisioned based on appropriate authorization by the service owner or delegate.	No deviation noted.
OG-8	Opsgenie Access is approved prior to provisioning access.	CC6.1 CC6.2 CC6.3	Inquired of the control owner and ascertained that access to Opsgenie systems was formally requested and approved prior to being provisioned as defined in the Atlassian's Standard Operating Procedure ("SOP") relating to User Provisioning Requests.	No deviation noted.
			Inspected a sample of users granted access to Opsgenie Systems and ascertained that a ticket was created and approved prior to the provisioning of access. Further ascertained that access granted was the same as access requested.	No deviation noted.

Access Management Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
IAM-11	The People Central Systems Support Specialist performs a review over Workday admin users semi-annually.	CC6.1 CC6.2 CC6.3	Inquired of the control owner and ascertained that the People Central Systems Support Specialist performed a review over Workday admin users semi-annually.	No deviation noted.
			Inspected a sampled user access review report over Workday Admin users and ascertained that the People Central Systems Support Specialist performed a review over Workday admin users on a semi-annual basis.	No deviation noted.
IAM-12	Bitbucket, Bitbucket Pipelines, Jira, Confluence, JSM and Insight, Forge, Data Lake, Compass Access to critical systems and services the Bitbucket Pipelines team uses to administer the service is reviewed semi-annually.	CC6.1 CC6.2 CC6.3	Inquired of the control owner and ascertained that administrative access to critical systems and services used by Bitbucket Pipelines was reviewed semi-annually.	No deviation noted.
			Inspected the sampled user access review and ascertained that administrative access to critical systems and services used by Bitbucket Pipelines was reviewed on a semi-annual basis.	No deviation noted.
IAM-13	Bitbucket, Bitbucket Pipelines, Jira, Confluence, JSM and Insight, Forge, Data Lake, Compass Privileged access to Deployment Bamboo is restricted to the members of the Build Engineering team.	CC2.1 CC6.1 CC6.2 CC6.3 CC6.8 CC8.1	Inquired of the control owner and ascertained that privileged access to Deployment Bamboo was restricted to the members of the Build Engineering team.	No deviation noted.
			Inspected the list of users with privileged access to Deployment Bamboo and ascertained that access was restricted to the members of the Build Engineering team.	No deviation noted.
IAM-14	Bitbucket, Bitbucket Pipelines, Jira, Confluence, JSM and Insight, Forge, Data Lake, Compass	CC6.3	Inquired of the control owner and ascertained that access to Artifactory was reviewed by the Build Engineering team on a semi-annual basis.	No deviation noted.

Access Management Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
	The Build Engineering team performs a semi-annual access review for Artifactory.		Inspected the sampled user access review and ascertained that access to Artifactory was reviewed by the Build Engineering team on a semi-annual basis.	No deviation noted.
IAM-15	JSM and Insight, and Bitbucket Pipelines Direct access to Kubernetes environments requires a valid key and two-factor authentication.	CC6.1 CC6.2 CC6.6	Inquired of the control owner and ascertained that direct access to the Kubernetes environments required a valid key and two-factor authentication.	No deviation noted.
			Inspected the network configuration and ascertained that direct access to the Kubernetes environments required a valid key and two-factor authentication.	No deviation noted.
			Attempted access to the Kubernetes environment with and without a valid SSH key and ascertained that a valid SSH key and two-factor authentication was required.	No deviation noted.
IAM-16	Administrative access to SSAM is provisioned based on appropriate authorization by the service owner or delegate.	CC6.1 CC6.2 CC6.3	Inquired of the control owner and ascertained that administrative access to SSAM was provisioned based on appropriate authorization by the service owner or delegate.	No deviation noted.
			Inspected the history log for a sample of admin user provisioned to SSAM and ascertained that administrative access to SSAM was provisioned based on appropriate authorization by the service owner or delegate.	No deviation noted.

Access Management Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
IAM-17	User access reviews for Kubernetes and SSAM containers are performed on a semi-annual basis and issues identified are remediated in a timely manner.	CC6.1 CC6.2 CC6.3	Inquired of the control owner and ascertained that access to critical supporting tools and services were reviewed semi-annually, and issues identified were remediated in a timely manner.	No deviation noted.
			Inspected the documentation of a sampled user access review and ascertained that a review of privileged user access for critical supporting tools and services was performed semi-annually. Issues identified were remediated in a timely manner.	SSAM User Access Review No deviation noted. Kubernetes User Access Review Deviation noted. For JSM and Insight and Bitbucket Pipelines, the sampled user access review was not complete and accurate as one (1) container used by Kubernetes was not reviewed.
Management Response: Atlassian determined that all relevant access were in fact reviewed at the time of the user access review, however it was not completely documented. The relevant team provided evidence of review, including logs showing access changes implemented as a result of the review. Atlassian has reinforced the requirements to the relevant team to ensure that future reviews are appropriately documented.				
IAM-18	Only service owners have the ability to grant and remove delegate access in SSAM.	CC6.1 CC6.2 CC6.3	Inquired of the control owner and ascertained that only service owners have the ability to grant and remove delegate access in SSAM.	No deviation noted.

Access Management Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
			Attempted to gain access to SSAM as a service owner and ascertained that only service owners of a SSAM container have the ability to grant and remove delegate access.	No deviation noted.
			Attempted to gain access to SSAM as a delegate and ascertained that granting and removing delegate access was not allowed.	No deviation noted.
			Attempted to gain access to SSAM as a user with no privileged role and ascertained that granting and removing delegate access was not allowed.	No deviation noted.
IAM-19	Only authorized service owners and delegates have the access to add, modify, and remove access in SSAM containers.	CC6.1 CC6.2 CC6.3	Inquired of the control owner and ascertained that only authorized service owners and delegates have the access to add, modify, and remove access in SSAM containers.	No deviation noted.
			Inspected the role of a service owner in a SSAM container and ascertained that service owners have access to add, modify, and remove access in the assigned SSAM container.	No deviation noted.
			Inspected the role of a delegate in a SSAM container and ascertained that delegates have access to add, modify, and remove access in the assigned SSAM container.	No deviation noted.
			Inspected the role of a user who is not a service owner or delegate in a SSAM container, and ascertained that users can only request for access, and do not have access to add, modify, and remove access in the assigned SSAM container.	No deviation noted.

Access Management Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
BBPL-18	Bitbucket (11/1/2020 to 8/26/2021) Physical access to the data centers housing Bitbucket cloud hardware is reviewed semi-annually.	CC6.4	Inquired of the control owner and ascertained that physical access to the data centers housing Bitbucket cloud hardware was reviewed semi-annually.	No deviation noted.
			Inspected the access listing of the production data centers and ascertained that physical access to the production data centers housing Bitbucket cloud hardware was reviewed semi-annually.	No deviation noted.

Incident Management, Backup, and Recovery Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
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 process must meet the Atlassian Incident Management Standard.	CC2.2 CC3.2 CC6.8 CC7.2 CC7.3 CC7.4 CC7.5	Inquired of the control owner and ascertained that incident management process was in place, with the Site Reliability team responsible for incidents and problems for Atlassian services and platforms, and that incident management process must have met the Atlassian Incident Management Standard. For incidents with severity level 0, 1, and 2, Root Cause Analysis was performed.	No deviation noted.
			Inspected a sample of incidents and issues from the incident reporting and tracking system, and ascertained that incidents and issues were monitored and resolved timely. If Jira ticket corresponded to severity level 0 and 1, ascertained that post incident review ("PIR") and root cause analysis were performed. If a Jira ticket corresponded to severity level 2 and 3, ascertained that post incident review express ("PIR-X") was performed.	No deviation noted.
BBPL-19	Bitbucket Bitbucket performs daily automated backups and annual restoration testing.	A1.2 A1.3 CC7.4 CC7.5	Inquired of the control owner and ascertained that daily automated backups and annual restoration testing was performed for Bitbucket.	No deviation noted.
			Inspected the configuration in Postgres SQL, NetApp, and S3, and ascertained that daily automated backups was performed for Bitbucket.	No deviation noted.

Incident Management, Backup, and Recovery Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
			Inspected the restoration testing reports, and supporting documentation of the annual restore test, and determined a restore test was successfully completed within the past year.	No deviation noted.
BBPL-20	Bitbucket Pipelines Bitbucket Pipelines data is backed up on a daily basis and is subject to annual restoration testing.	A1.2 A1.3 CC7.4 CC7.5	Inquired of control owner and ascertained that Bitbucket Pipelines data was backed up on a daily basis and was subjected to annual restoration testing.	No deviation noted.
			Inspected the configuration in S3 and ascertained that Bitbucket Pipelines data was automatically backed up on a daily basis.	No deviation noted.
			Inspected the restoration testing reports, and supporting documentation of the annual restore test, and determined a restore test was successfully completed within the past year.	No deviation noted.
OG-9	Opsgenie Opsgenie performs frequent, automatic backups, replication and routine restore testing.	A1.2 A1.3 CC7.4 CC7.5	Inquired of the control owner and ascertained that Opsgenie data was routinely backed up and replicated across multiple regions.	No deviation noted.
			Inspected the replication configuration, and ascertained that AWS was configured to perform real-time automatic replication.	No deviation noted.
			Inspected a sample of quarterly restoration testing results and ascertained that routine restore testing was performed successfully. Further ascertained that any issues identified from the restoration testing were investigated and resolved timely.	No deviation noted.

Incident Management, Backup, and Recovery Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
BBPL-21	Bitbucket PostgreSQL data is replicated in real time from its primary site to a secondary site.	A1.2 A1.3 CC7.4 CC7.5	Inquired of the control owner and ascertained that PostgreSQL data was replicated in real time from its primary site to a secondary site.	No deviation noted.
			Inspected the configuration of the replication and ascertained that PostgreSQL data was replicated in real time from its primary site to a secondary site.	No deviation noted.
BBPL-22	Bitbucket Bitbucket production data is replicated every 2 hours from its primary site to a secondary site.	A1.2 A1.3 CC7.4 CC7.5	Inquired of the control owner and ascertained that Bitbucket production data in NetApp was replicated every 2 hours from its primary site to a secondary site.	No deviation noted.
			Inspected the configuration in NetApp and ascertained that Bitbucket production data in NetApp was replicated every 2 hours from its primary site to a secondary site.	No deviation noted.
BBPL-23	Bitbucket Replication is monitored for failures and an alert is created and resolved.	A1.2 A1.3 CC7.4 CC7.5	Inquired of the control owner and ascertained that replication was monitored for failures and an alert was created and resolved.	No deviation noted.
			Inspected the replication and alert configuration from the monitoring tool and ascertained that replication was monitored for failures and an alert was created and resolved.	No deviation noted.
			Inspected a sample of incidents and issues from the incident reporting and tracking system and ascertained that incidents and issues were monitored and resolved timely.	No deviation noted.
PL-7	Jira, Confluence, JSM and Insight, Forge, Compass, and Data Lake	A1.2 A1.3 CC7.4 CC7.5	Inquired of the control owner and ascertained that replication and backups were in place to provide data redundancy and availability for Micros.	No deviation noted.

Incident Management, Backup, and Recovery Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
	Replication and backups are in place to provide data redundancy and availability for Micros.		Inspected the replication configuration and ascertained that the replications were configured real time from the primary site to a secondary site.	No deviation noted.
			Inspected a sample of quarterly restoration testing for the Micros Platform and ascertained that routine restore testing was performed successfully. Further ascertained that any issues identified from the restoration testing were investigated and resolved timely.	Confluence, JSM and Insight, Forge, Compass, and Data Lake No deviation noted. Jira Deviation noted. For Jira, two (2) of two (2) sampled quarterly backup restorations were not completed for a component of Jira called Automation for Jira (AFJ).
Management Response: The issue is related to a specific component of Jira, Automation for Jira (A4J). Atlassian has since performed a backup restoration test on November 15, 2021 which confirmed the recoverability of backups and has also automated the process to facilitate timely testing in the future.				
PL-8	JSM and Insight, and Bitbucket Pipelines Kubernetes clusters are replicated across multiple availability zones.	A1.2 A1.3 CC7.4 CC7.5	Inquired of the control owner and ascertained that Kubernetes clusters were replicated across multiple availability zones.	No deviation noted.

Incident Management, Backup, and Recovery Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
			Inspected the configuration in AWS and ascertained that Kubernetes clusters were replicated across multiple availability zones to permit the resumption of critical operations in the event of loss of a critical facility.	No deviation noted.
DR-1	A disaster recovery policy is in place and is reviewed on an annual basis by the disaster recovery steering committee.	A1.2 A1.3 CC7.4 CC7.5 CC9.1	Inquired of the control owner and ascertained a disaster recovery policy was in place and was reviewed on an annual basis by the disaster recovery steering committee.	No deviation noted.
			Inspected and observed the disaster recovery policy and ascertained that disaster recovery policy was in place and reviewed on an annual basis by the disaster recovery steering committee.	No deviation noted.
BBPL-24	Bitbucket A formal disaster recovery plan is in place for Bitbucket which is tested on an annual basis.	A1.2 A1.3 CC7.4 CC7.5 CC9.1	Inquired of the control owner and ascertained the formal disaster recovery plan was in place for Bitbucket which was tested on an annual basis.	No deviation noted.
			Inspected the disaster recovery plan and ascertained that the formal disaster recovery plan was in place for Bitbucket which was tested on an annual basis.	No deviation noted.
PL-9	Jira, Confluence, JSM and Insight, Opsgenie, Bitbucket Pipelines, Compass, Forge, and Data Lake A formal disaster recovery plan is in place for Jira, Confluence,	A1.2 A1.3 CC7.4 CC7.5 CC9.1	Inquired of the control owner and ascertained a formal disaster recovery plan was in place for Jira, Confluence, JSM and Insight, Opsgenie, Bitbucket Pipelines, Compass, Forge, and Data Lake, which was tested on a quarterly basis.	No deviation noted.

Incident Management, Backup, and Recovery Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
	JSM and Insight, Opsgenie, Bitbucket Pipelines, Compass, Forge, and Data Lake, which is tested on a quarterly basis.		Inquired of the control owner and ascertained a formal disaster recovery plan was in place for Jira, Confluence, JSM and Insight, Opsgenie, Bitbucket Pipelines, Compass, Forge, and Data Lake, which was tested on a quarterly basis.	No deviation noted.
			Inspected a sample of quarterly disaster recovery testing and ascertained that formal disaster recovery testing was performed timely.	No deviation noted.

Data Classification & Data Security Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
BBPL-25	Bitbucket External users connect to Bitbucket using encrypted traffic via SSH and TLS certificates. Certificates are rotated and reviewed prior to expiration.	C1.1 CC6.1 CC6.6 CC6.7	Inquired of the control owner and ascertained that external users connected to Bitbucket used encrypted traffic via SSH and TLS certificates. Additionally, ascertained that certificates were rotated and reviewed prior to expiration.	No deviation noted.
			Inspected the Bitbucket webpage and ascertained that external users connected to Bitbucket used encrypted traffic via SSH and TLS protocol, and certificates were reviewed prior to expiration.	No deviation noted.
BBPL-26	Bitbucket Pipelines Bitbucket Pipelines data is encrypted at rest.	C1.1 CC6.1 CC6.6 CC6.7	Inquired of the control owners that encryption at rest was enabled for all persistent data stores containing Bitbucket Pipelines data.	No deviation noted.
			Inspected the AWS configuration and ascertained that encryption at rest was enabled for DynamoDB, S3 and Elasticsearch data stores.	No deviation noted.
			Inspected a sample Bitbucket Pipelines data and ascertained that encryption at rest was enabled.	No deviation noted.
OG-10	Opsgenie External users securely connect to Opsgenie via the encrypted TLS protocol.	C1.1 CC6.1 CC6.6 CC6.7	Inquired of the control owner and ascertained that external users were connected to Opsgenie via the encrypted TLS protocol.	No deviation noted.
			Inspected the Opsgenie webpage and ascertained that external users were connected to Opsgenie using encrypted traffic via TLS protocol, and certificates were monitored for expiration via AWS.	No deviation noted.

Data Classification & Data Security Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
OG-11	Opsgenie Opsgenie data is encrypted at rest.	C1.1 CC6.1 CC6.6 CC6.7	Inquired of the control owner and ascertained that Opsgenie data was encrypted at rest.	No deviation noted.
			Inspected the AWS encryption configuration and ascertained that Opsgenie data was encrypted at rest.	No deviation noted.
PL-10	Jira and Confluence Data that contains attachment contents are encrypted.	C1.1 CC6.1 CC6.6 CC6.7	Inquired of the control owner and ascertained that external users were connected to Opsgenie via the encrypted TLS protocol.	No deviation noted.
			Inspected the Opsgenie webpage and ascertained that external users were connected to Opsgenie using encrypted traffic via TLS protocol, and certificates were monitored for expiration via AWS.	No deviation noted.
PL-11	Jira, Confluence, JSM and Insight, Compass, Forge, and Data Lake Data is encrypted at rest using AES-256 encryption algorithm.	C1.1 CC6.1 CC6.6 CC6.7	Inquired of the control owner and ascertained that Jira, Confluence, JSM and Insight, Compass, Forge, and Data Lake data was encrypted at rest using AES-256 server-side encryption.	No deviation noted.
			Inspected the AWS encryption configuration and ascertained that Micros, Jira, Confluence, JSM and Insight, Compass, Forge, and Data Lake data were encrypted at rest using AES-256 encryption.	No deviation noted.
PL-12	Jira, Confluence, JSM and Insight, Compass, Forge, and Data Lake External users connect to the Systems using encrypted traffic via TLS protocol. Certificates are rotated when required.	C1.1 CC6.1 CC6.6 CC6.7	Inquired of the control owner and ascertained the external users were connected to Jira, Confluence, JSM and Insight, Compass, Data Lake, and Forge using encrypted traffic via TLS protocol, and certificates were rotated when required.	No deviation noted.

Data Classification & Data Security Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
			Inspected the Jira, Confluence, JSM and Insight, Compass, Data Lake, and Forge webpages and ascertained the external users were connected to Jira, Confluence, JSM and Insight, Compass, Data Lake, and Forge using encrypted traffic via TLS protocol, and certificates were rotated when required.	No deviation noted.
BBPL-27	Bitbucket and Bitbucket Pipelines Firewall rules are in place to restrict access to the Bitbucket Cloud production environment.	CC6.6 CC6.7	Inquired of the control owner and ascertained firewall rules were in place to restrict access to the Bitbucket Cloud production environment.	No deviation noted.
			Inspected the security policy settings and the configurations set up, and ascertained firewall rules were in place to restrict access to the Bitbucket Cloud production environment.	No deviation noted.
OG-12	Opsgenie Firewall rules are in place to restrict access to the Opsgenie production environment.	CC6.6 CC6.7	Inquired of the control owner and ascertained firewall rules specific to Opsgenie were in place to restrict access to the production environment.	No deviation noted.
			Inspected the security policy settings and the configurations set up in the AWS Console, and ascertained that firewall rules were in place to restrict access to the Opsgenie production environment.	No deviation noted.
PL-13	Jira, Confluence, JSM and Insight, Compass, Forge, and Data Lake Firewalls rules are in place and are configured using security	CC6.6 CC6.7	Inquired of the control owner and ascertained that firewall rules were in place and were configured using security policy rules to limit unnecessary ports, protocols, and services, and maintained by the Micros team.	No deviation noted.

Data Classification & Data Security Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
	policy rules to limit unnecessary ports, protocols, and services and maintained by the Micros team. All changes to firewall rules require a peer reviewed pull request.		Inspected the security policy settings and the configurations set up in AWS, and ascertained firewall rules were in place to limit unnecessary ports, protocols, and services.	No deviation noted.
			Inspected the firewall rules and ascertained that the firewall rules resided in Bitbucket and changes to the firewall rules required a peer reviewed pull request prior to deployment.	No deviation noted.
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.	C1.1 CC6.6 CC6.7	Inquired of the control owner and ascertained that production data is not used in non-production environments. If production data was used in non-production environments, the data must be protected in alignment with Atlassian's System Acquisition, Development, and Maintenance Policy.	No deviation noted.
			Inspected the 'System Acquisition, Development, and Maintenance' Policy documented in the Confluence page under the 'Test Data Policy' section and ascertained the production data was not used in non-production environments and production data was anonymized or masked if used in pre-production environments.	No deviation noted.
			Inspected a sample of customer's production data in the production environment and ascertained that the customer's production data does not exist in the non-production environment.	No deviation noted.
DS-2	Data is classified according to company policy.	C1.1 C1.2	Inquired of the control owner and ascertained data was classified according to company policy.	No deviation noted.

Data Classification & Data Security Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
			Inspected the company policy and ascertained that data classification level was documented within the policy.	No deviation noted.
			Inspected a sample of each data classification type and ascertained that it was assigned a classification level according to Atlassian's Data Security and Information Lifecycle Management Policy.	No deviation noted.
DS-3	A ZeroTrust infrastructure is implemented to place endpoints into a tiered network (High, Low, Open) based on their security posture and type of device. Applications added to the SSO platform are tiered according to the ZeroTrust policy. Endpoints cannot access applications via the SSO platform unless they are placed on the same/higher tier as the application.	CC6.6 CC6.7	Inquired of the control owner and ascertained that a ZeroTrust Network was implemented to manage and protect network infrastructure and network services. Further ascertained that known devices were enrolled into Atlassian's management platform and services were placed into tiers to further restrict access. Any changes to the ZeroTrust settings required a peer review.	No deviation noted.
			Inspected the ZeroTrust Service Tier policy and ascertained that service tiers were documented and defined.	No deviation noted.
			Inspected the ZeroTrust Posture page and ascertained that registered known devices were enrolled. Further ascertained that compliance checks were performed on devices and access to the service tiers were based on the devices.	No deviation noted.
			Inspected a sample of service tier and ascertained that access to the services were restricted based on the known devices registered in ZeroTrust.	No deviation noted.

Data Classification & Data Security Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
BBPL-28	Bitbucket Equipment is decommissioned and the data residing on the hardware is sanitized or destroyed.	C1.2	Inquired of the control owner and ascertained that equipment was decommissioned and the data residing on the hardware was sanitized or destroyed.	No deviation noted.
			Inspected evidence of a sample of equipment that was decommissioned and ascertained that data residing on the hardware was sanitized or destroyed.	No deviation noted.

Vulnerability & Network Security Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
OG-13	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.	A1.1 CC2.2 CC2.3 CC3.2 CC7.1 CC7.2	Inquired with the control owner and ascertained that AWS CloudWatch was in place to track and notify on the availability, reliability, and processing capacity of Opsgenie systems and core services.	No deviation noted.
			Inspected the configuration of the monitoring thresholds in AWS CloudWatch and ascertained that the monitoring of availability and processing capacity of Opsgenie systems and core services were tracked and monitored.	No deviation noted.
			Inspected the configuration of the alert notification in AWS CloudWatch, and ascertained that alerts were sent to the on-call engineers in an event an availability or processing capacity issues were detected.	No deviation noted.
			Inspected a sample of availability and processing capacity and issues from the incident reporting and tracking system, and ascertained that incidents and issues were monitored and resolved timely.	No deviation noted.
			Inspected a sample of quarterly capacity audit and load test results and ascertained that system-wide capacity audits were performed quarterly relating to Opsgenie to determine the current and future resources needed to meet customer expectations of the goods and services being delivered.	No deviation noted.

Vulnerability & Network Security Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
PL-14	Jira, Confluence, JSM and Insight, Compass, Forge, 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.	A1.1 CC2.2 CC2.3 CC3.2 CC7.1 CC7.2	Inquired of the control owner and ascertained that monitoring uses were used to monitor the availability and capacity of Jira, Confluence, JSM and Insight, Compass, Forge, and Data Lake. Further ascertained that alerts were automatically sent to on-call engineers and changes to availability were published online so that customers may check the status of Jira, Confluence, JSM and Insight, Compass, Forge, and Data Lake.	No deviation noted.
			Inspected the monitoring tools and ascertained that Jira, Confluence, JSM and Insight, Compass, Forge, and Data Lake used tools to monitor the availability and processing capacity of each services. When issues are detected, alerts are automatically sent to on-call engineers and resolved as necessary. Further ascertained that the incident management procedure was followed when availability and processing capacity issues were identified.	No deviation noted.
			Inspected Atlassian's client facing webpage and ascertained that major changes to availability were published online so that customers may check the status of Jira, Confluence, JSM and Insight, Compass, Forge, and Data Lake.	No deviation noted.
PL-15	JSM and Insight, and Bitbucket Pipelines Kubernetes uses AWS Autoscaling to automatically	CC2.3 A1.1 A1.2	Inquired of the control owner and ascertained that AWS Autoscaling was used for Kubernetes to automatically adjust the capacity of the platform.	No deviation noted.

Vulnerability & Network Security Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
	adjust the capacity of the platform.		Inspected the configuration of AWS Autoscaling and ascertained that autoscaling was enabled on all clusters to automatically adjust the capacity of the Kubernetes platform.	No deviation noted.
BBPL-29	Bitbucket Monitoring tools are in place to track and notify on the availability and reliability of Bitbucket Cloud systems and services.	A1.1 CC2.3 CC3.2 CC7.1 CC7.2	Inquired of the control owner and ascertained that monitoring tools were in place to track and notify on the availability and reliability of Bitbucket Cloud systems and services.	No deviation noted.
			Inspected the monitoring tools in place and ascertained that monitoring tools SignalFX, Pollinator, and Splunk were in place to track and notify on the availability and reliability of Bitbucket Cloud systems and services.	No deviation noted.
BBPL-30	Bitbucket Bitbucket Cloud uses tools to monitor the availability of customer-facing services. The availability is published so that customers may check the status/uptime of Bitbucket Cloud.	A1.1 CC2.3 CC3.2 CC7.1 CC7.2	Inquired of the control owner and ascertained that Bitbucket Cloud used tools to monitor the availability of customer-facing services. The availability was published so that customers could check the status/uptime of Bitbucket Cloud.	No deviation noted.
			Inspected the monitoring tools in place and the customer-facing external website and ascertained that Bitbucket Cloud used tools to monitor the availability of customer-facing services. Additionally, ascertained that the availability was published so that customers could check the status/uptime of Bitbucket Cloud.	No deviation noted.

Vulnerability & Network Security Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
BBPL-31	Bitbucket Pipelines Monitoring tools are in place to track and notify on the availability and reliability of Bitbucket Pipelines services.	A1.1 CC2.3 CC3.2 CC7.1 CC7.2	Inquired of the control owner and ascertained that monitoring tools were in place to track and notify on the availability and reliability of Bitbucket Pipelines services.	No deviation noted.
			Inspected the monitoring tools in place and ascertained that monitoring tools SignalFX, Opsgenie, and Slack were in place to track and notify on the availability and reliability of Bitbucket Pipelines services.	No deviation noted.
OG-14	Opsgenie Opsgenie publishes availability so customers can check status and uptime metrics.	A1.1 CC2.3 CC3.2	Inquired of the control owner and ascertained that availability was published in the customer facing website so that customers could check the status and uptime of Opsgenie.	No deviation noted.
			Inspected the customer facing website and ascertained that availability was published real-time, and the status and uptime metrics were communicated to customers.	No deviation noted.
MTR-1	Atlassian uses malware protection for Windows and OSX clients. An enterprise anti-malware platform provides endpoint protection, centralized reporting, and notifications. The client is installed via management platforms and protected by a complex password to prevent staff from removing or uninstalling the agent.	CC3.2 CC6.1 CC6.7 CC6.8	Inquired of the control owner and ascertained that malware protection for Windows and OSX clients was implemented, and security patching was enforced on Windows endpoints. Additionally, complex password on the management platform prevented Windows and OSX clients from removing or uninstalling the agent.	No deviation noted.
			Inspected the configuration settings in the software used to enforce Malware protection and ascertained that malware protection was implemented and security patching was enforced on Windows endpoints.	No deviation noted.

Vulnerability & Network Security Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
			Attempted to uninstall the Malware protection software and ascertained that the malware protection was configured to prevent any users to uninstall the software.	No deviation noted.
MTR-2	Continuous vulnerability scanning is performed over the Atlassian environment. Vulnerabilities are reviewed, prioritized, and resolved as per the defined timeframe.	CC3.2 CC7.1 CC7.2 CC7.3 CC7.4	Inquired of the control owner and ascertained that continuous vulnerability scanning was performed over the Atlassian environment. Vulnerabilities were reviewed, prioritized, and resolved as per the defined timeframe.	No deviation noted.
			Inspected the configuration and tool used to monitor vulnerabilities and ascertained that technical vulnerability management was implemented using vulnerability scanners, and critical threats were reviewed, prioritized, and resolved as per the defined timeframe by the security team.	No deviation noted.
			Inspected a sample of vulnerabilities identified from the vulnerability scanners and ascertained that incidents and issues were reviewed, prioritized, and resolved as per the defined timeline by the security team.	No deviation noted.
MTR-3	Penetration testing is performed by Bug Bounty on a continuous basis. Issues are reviewed, prioritized, and resolved within the defined timeframe.	CC3.2 CC7.1 CC7.2 CC7.3 CC7.4	Inquired of the control owner and ascertained that penetration testing was performed by Bug Bounty on a continuous basis, and that issues were reviewed, prioritized, and resolved within the defined timeframe.	No deviation noted.

Vulnerability & Network Security Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
			Inspected the configuration of the BugCrowd application and observed that it ran on a continuous basis, and issues were automatically created in a Jira ticket and tracked to completion by the Security team.	No deviation noted.
			Inspected a sample of issues identified from the penetration testing and ascertained that issues were reviewed and tracked to completion in a Jira ticket within the defined timeframe by the Security team.	No deviation noted.
MTR-4	IT asset management software is used to enforce hard drive encryption, user authentication requirements, and security patching on MacOS endpoints.	CC3.2 CC6.1 CC6.7 CC6.8	Inquired of the control owner and ascertained that IT asset management software was used to enforce hard drive encryption, user authentication requirements, and security patching on MacOS endpoints.	No deviation noted.
			Inspected the software used to enforce encryption and ascertained that IT Asset management software was used to enforce hard drive encryption, user authentication requirements, and security patching was enforced on MacOS endpoints.	No deviation noted.
MTR-5	IT Asset management software is used to monitor hard drive encryption, user authentication requirements, and security patching on Windows endpoints.	CC3.2 CC6.1 CC6.7 CC6.8 CC7.1	Inquired of the control owner and ascertained that IT asset management software was used for monitoring hard drive encryptions, user authentication requirements, and security patching on Windows endpoints.	No deviation noted.

Vulnerability & Network Security Controls

Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
			Inspected the software used to enforce encryption and ascertained that IT Asset management software was used to monitor the hard drive encryption, user authentication requirements, and security patching was enforced on Windows endpoints.	No deviation noted.
MTR-6	Code scanning is performed on a continuous basis. Vulnerabilities are reviewed periodically and resolved within Atlassian's standard resolution timeframes.	CC6.8 CC7.1	Inquired of the control owner and ascertained that code scanning was performed on a continuous basis. Vulnerabilities were reviewed periodically and resolved within Atlassian's standard resolution timeframes.	No deviation noted.
			Inspected the configuration of the SourceClear code scan and ascertained that it ran on a continuous basis. Further inspected the configuration between the code scanning tool and the Atlassian Platform products and ascertained that SourceClear scans every time a code is merged.	No deviation noted.
			Inspected a sample of vulnerabilities identified from the code scanning on Atlassian Platform source codes ascertained that vulnerabilities were reviewed periodically and resolved within Atlassian's standard resolution timeframes.	Jira, Confluence, JSM and Insight, Forge, Compass, and Data Lake No deviation noted. Opsgenie Deviation noted. For Opsgenie, three (3) of the 25 sampled vulnerabilities identified by

Vulnerability & Network Security Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
				SourceClear, the vulnerabilities were not resolved timely based on the SLA policy of six (6) weeks.

Management Response:
Atlassian has reviewed the vulnerabilities for Opsgenie and determined that there was no security impact from the delay in the remediation. Atlassian has improved employee awareness over the vulnerability remediation process and assigned security champions to monitor due dates.

Vendor Management Controls				
Control #	Controls Specified by Atlassian	Criteria	Tests of Controls	Results of Test
VDR-1	Vendor agreements, including any security, availability, and confidentiality commitments, are reviewed during the procurement process.	C1.1 C1.2 CC1.1 CC1.3 CC1.4 CC2.3 CC3.4 CC9.2	Inquired of the control owner and ascertained that vendor agreements, including any security, availability, and confidentiality commitments, were reviewed during the procurement process.	No deviation noted.
			Inspected a sample of new vendors' third-party contracts and ascertained that the contracts include security, availability, and confidentiality commitments, and the contracts were executed between the third-party and Atlassian during the procurement process.	No deviation noted.
VDR-2	Atlassian reviews the SOC reports of the vendors on an annual basis.	A1.2 C1.1 C1.2 CC1.3 CC2.3 CC6.1 CC6.4 CC6.5 CC9.2	Inquired of the control owner and ascertained that Atlassian reviewed the SOC reports of the vendors on an annual basis.	No deviation noted.
			Inspected the Jira ticket for the review of the SOC 2 or equivalent attestation reports and ascertained that leadership reviewed the reports annually. Reviews included an assessment of complementary user entity controls, subservice organizations, and mapping of the controls to key risks. If there were exceptions, Atlassian reviewed the severity and impact of the exceptions, and if needed, followed-up with the individual vendor.	No deviation noted.

Atlassian's Platform Controls Mapped to the Security, Confidentiality, and Availability Criteria

Criteria	Criteria Description	Supporting Control
CC 1.0 Common Criteria Related to Control Environment		
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	ELC-3, ELC-8, ELC-5, ELC-10, HR-5, HR-7, VDR-1
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	ELC-8, ELC-5, ELC-4, ELC-7, ELC-6, RM-1, BBPL-28
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	ELC-8, ELC-5, VDR-1, VDR-2, HR-1, ELC-2, ELC-1
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	ELC-3, ELC-8, ELC-5, VDR-1, HR-2, HR-3, HR-9, HR-7, HR-8
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	ELC-3, ELC-8, HR-4, HR-5, HR-7, HR-8
CC 2.0 Common Criteria Related to Communication and Information		
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	ELC-8, ELC-4, ELC-7, ELC-6, ELC-9, RM-3, RM-4, CHG-1, CHG-2, CHG-3, CHG-4, CHG-6, CHG-10, IAM-9, IAM-13, CHG-11, CHG-5, CHG-7, CHG-9, CHG-8, MICROS-1, PL-5, MICROS-2, BBPL-8, BBPL-9, BBPL-10, OG-4, OG-5
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	HR-4, HR-5, HR-6, HR-9, ELC-8, ELC-12, CMC-6, IM-1, CMC-2, CMC-4, CMC-5, CMC-1, OG-13, PL-14

Criteria	Criteria Description	Supporting Control
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	ELC-8, ELC-4, ELC-7, ELC-6, RM-3, ELC-12, VDR-1, VDR-2, CMC-3, CMC-6, CMC-2, CMC-5, CMC-4, CMC-1, OG-13, PL-14, PL-15, BBPL-29, BBLP-30, OG-14, BBPL-31
CC 3.0 Common Criteria Related to Risk Assessment		
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	RM-2, RM-1, RM-4, ELC-8, RM-3, ELC-9, ELC-13, ELC-11
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	RM-2, RM-1, RM-4, RM-3, IM-1, MTR-1, MTR-4, MTR-3, MTR-5, CMC-1, MTR-2, OG-13, PL-14, BBPL-29, BBLP-30, OG-14, BBPL-31
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	RM-3
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	ELC-4, ELC-7, ELC-6, RM-1, VDR-1
CC 4.0 Common Criteria Related to Monitoring Activities		
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.	RM-2, RM-1, RM-4, ELC-8
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-2, RM-1, RM-4, ELC-8
CC 5.0 Common Criteria Related to Control Activities		
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-2, RM-1, RM-4, RM-3

Criteria	Criteria Description	Supporting Control
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	RM-2, RM-1, RM-4, ELC-8, RM-3
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	RM-2, RM-1, RM-4, ELC-3, HR-2, HR-8, HR-7
CC 6.0 Common Criteria Related to Logical and Physical Access Controls		
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	IAM-1, IAM-2, IAM-3, IAM-4, IAM-5, IAM-13, IAM-6, IAM-8, IAM-7, IAM-11, IAM-9, CHG-11, MTR-1, MTR-4, MTR-5, VDR-2, IAM-12, IAM-10, BBPL-3, BBPL-4, BBPL-5, OG-2, PL-2, PLATO-1, BBPL-6, OG-3, PL-3, BBPL-7, PL-4, MICROS-3, MICROS-4, BBPL-11, BBPL-12, MICROS-6, BBPL-13, OG-6, PL-6, BBPL-14, OG-7, BBPL-15, BBPL-16, OG-8, IAM-15, IAM-16, IAM-17, IAM-18, IAM-19, BBPL-25, BBPL-26, OG-10, OG-11, PL-10, PL-11, PL-12, DTL-1
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.	IAM-1, IAM-2, IAM-5, IAM-3, IAM-13, CHG-11, IAM-6, IAM-8, IAM-7, IAM-11, IAM-9, IAM-12, IAM-10, BBPL-3, BBPL-4, BBPL-5, OG-2, PL-2, PLATO-1, BBPL-7, PL-4, MICROS-3, MICROS-4, MICROS-5, BBPL-11, BBPL-12, MICROS-6, BBPL-13, OG-6, PL-6, BBPL-14, OG-7, BBPL-15, BBPL-16, BBPL-17, OG-8, IAM-15, IAM-16, IAM-17, IAM-18, IAM-19, DTL-1

Criteria	Criteria Description	Supporting Control
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.	IAM-3, IAM-4, IAM-13, CHG-11, IAM-6, IAM-9, IAM-14, IAM-12, IAM-10, BBPL-3, BBPL-4, BBPL-5, OG-2, PL-2, PLAT0-1, MICROS-3, MICROS-4, MICROS-5, BBPL-11, BBPL-12, MICROS-6, BBPL-13, OG-6, PL-6, BBPL-14, OG-7, BBPL-15, BBPL-17, OG-8, IAM-11, IAM-16, IAM-17, IAM-18, IAM-19, DTL-1
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	BBPL-18, VDR-2
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.	BBPL-1, VDR-2, BBPL-2, OG-1, PL-1
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	IAM-1, IAM-2, IAM-3, DS-3, DS-1, BBPL-6, OG-3, PL-3, MICROS-3, BBPL-11, BBPL-15, IAM-15, BBPL-25, BBPL-26, OG-10, OG-11, PL-10, PL-11, PL-12, BBPL-27, OG-12, PL-13
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.	DS-1, BBPL-1, MTR-1, MTR-4, MTR-5, DS-3, BBPL-2, OG-1, PL-1, BBPL-6, OG-3, PL-3, BBPL-25, BBPL-26, OG-10, OG-11, PL-10, PL-11, PL-12, BBPL-27, OG-12, PL-13
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.	CHG-1, CHG-2, CHG-3, CHG-4, CHG-5, CHG-6, CHG-10, IAM-13, CHG-11, MTR-1, MTR-4, MTR-5, CMC-6, IM-1, CHG-7, CHG-9, CHG-8, MICROS-1, PL-5, MICROS-2, BBPL-8, BBPL-9, BBPL-10, OG-4, OG-5, MTR-6

CC7.0 Common Criteria Related to System Operations		
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.	OG-13, MTR-5, MTR-3, MTR-2, PL-14, BBPL-29, BBLP-30, BBPL-31
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	MTR-3, MTR-2, IM-1, OG-13, PL-14, BBPL-29, BBLP-30, BBPL-31
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.	MTR-3, MTR-2, IM-1
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.	ELC-3, CMC-5, MTR-3, MTR-2, IM-1, CMC-6, DR-1, BBPL-19, BBPL-20, OG-9, BBPL-21, BBPL-22, BBPL-23, PL-7, PL-8, BBPL-24, PL-9
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	CMC-5, IM-1, CMC-6, DR-1, BBPL-19, BBPL-20, OG-9, BBPL-21, BBPL-22, BBPL-23, PL-7, PL-8, BBPL-24, PL-9
CC 8.0 Common Criteria Related to Change Management		
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	CHG-1, CHG-2, CHG-3, CHG-4, CHG-5, CHG-6, CHG-10, CHG-11, IAM-13, IAM-9, CHG-7, CHG-9, CHG-8, MICROS-1, PL-5, MICROS-2, BBPL-8, BBPL-9, BBPL-10, OG-4, OG-5

CC 9.0 Common Criteria Related to Risk Mitigation		
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	RM-2, RM-1, DR-1, BBPL-24, PL-9
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	VDR-1, VDR-2
A 1.0 Additional Criteria for Availability Criteria		
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.	MGRT-1, OG-13, PL-14, PL-15, BBPL-29, BBLP-30, OG-14, BBPL-31
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	BBPL-14, BBPL-19, BBPL-20, DR-1, VDR-2, OG-9, BBPL-21, BBPL-22, BBPL-23, PL-7, PL-8, BBPL-24, PL-9, PL-15
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	BBPL-19, BBPL-20, DR-1, OG-9, BBPL-21, BBPL-22, BBPL-23, PL-7, PL-8, BBPL-24, PL-9
C 1.0 Additional Criteria for Confidentiality Criteria		
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	DS-1, DS-2, BBPL-1, VDR-1, VDR-2, BBPL-2, OG-1, PL-1, BBPL-6, OG-3, PL-3, MICROS-4, BBPL-25, BBPL-26, OG-10, OG-11, PL-10, PL-11, PL-12
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	DS-2, BBPL-1, VDR-1, VDR-2, BBPL-2, OG-1, PL-1