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

Atlassian PTY Ltd.

System and Organization Controls (SOC) 3 Report

Report on Atlassian Platform

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

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

Table of Contents
Atlassian Platform

Section I: Atlassian's Management Assertion

ATLASSIAN

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

We, as management of, Atlassian PTY Ltd. ("Atlassian") are responsible for:

- Identifying the Atlassian Platform (System) and describing the boundaries of the System, which are presented in Attachment A
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system, which are presented in Attachment B
- identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the principal service commitments and system requirement
- Selecting the trust services categories that are the basis of our assertion

We assert that the controls over the system were effective throughout the period November 1, 2020 to September 30, 2021, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, and confidentiality set forth in the AICPA's TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

Subservice Organizations Matters
Atlassian uses Amazon Web Services ("AWS") 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 System (Attachment A) 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.

However, we perform annual due diligence procedures for third-party sub-service providers and based on the procedures performed, nothing has been identified that prevents Atlassian from achieving its specified service commitments.

Very truly yours,

DocuSigned by:
88C748362EA44C0...

Adrian Ludwig
Chief Trust Officer, Atlassian

Section II: Independent Service Auditor's Opinion

Building a better
working world

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

Tel: +1 408 947 5500
Fax: +1 408 947 5717
ey.com

Report of Independent Accountants

To the Management of Atlassian Pty Ltd.

Scope

We have examined management's assertion, contained within the accompanying Management's Report of its Assertions on the Effectiveness of Its Controls Over the Atlassian Platform System Based on the Trust Services Criteria for Security, Availability, and Confidentiality (Assertion), that Atlassian's controls over the Atlassian Platform (System) were effective throughout the period November 1, 2020 to September 30, 2021, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Atlassian Pty Ltd ("the Company" or "Atlassian") uses Amazon Web Services ("AWS") 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 of the boundaries of the System (Attachment A) indicates that Atlassian controls can provide reasonable assurance that certain service commitments and system requirements, based on the applicable trust services criteria, can be achieved only if AWS and NTT 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 presents Atlassian's system and the types of 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.

Management's Responsibilities

Atlassian's management is responsible for its assertion, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the Atlassian Platform (System) and describing the boundaries of the System
- Identifying our principal service commitments and system requirements and the risks that would threaten the achievement of the principal service commitments and service requirements that are the objectives of our system

- identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the principal service commitments and system requirement

Our Responsibilities

Our responsibility is to express an opinion on the Assertion, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Atlassian's relevant security, availability, and confidentiality policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Atlassian's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Inherent limitations

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve Atlassian's principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Opinion

In our opinion, Atlassian's management assertion referred to above is fairly stated, in all material respects, based on the security, availability, and confidentiality criteria (applicable trust services criteria), and if the subservice organizations applied the controls assumed in the design of Atlassian's controls throughout the period November 1, 2020 to September 30, 2021.

Ernst + Young LLP

December 9, 2021

Section III: Attachment A – Atlassian Service Organization's Description of the Boundaries of the System

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

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 20, 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).

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)
	Redis	Opsgenie, Bitbucket Cloud (Pre-Migration), Bitbucket Pipelines, and Forge

Component	Service Provider	Products
	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
Messaging	Amazon Simple Queue Service (SQS)	Jira Cloud, Confluence Cloud, JSM, Compass, Bitbucket Pipelines, Forge, and Opsgenie

Component	Service Provider	Products
	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 Cloud (Pre-Migration and Post-Migration), Bitbucket Pipelines, Forge, and Compass

Component	Service Provider	Products
	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-Migration), Bitbucket Pipelines, Forge, and Compass

Component	Service Provider	Products
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:

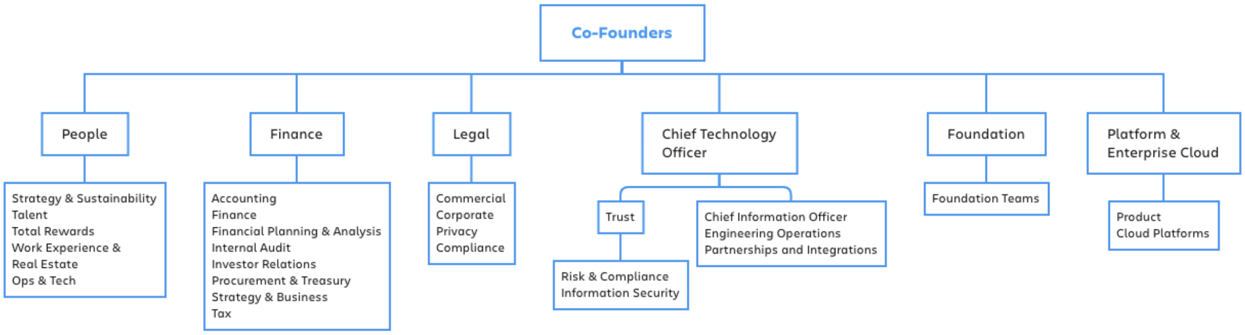

Figure 2: Atlassian's Organizational Chart

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.

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

Criteria	Service Organization	Controls
		control cards. Additional security 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.

Criteria	Service Organization	Controls
A1.2: The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	AWS NTT	Environmental protections have been installed including the following: • Cooling systems • Battery and generator backups • Smoke detection • Dry pipe sprinklers Environmental protection equipment receives maintenance on at least an annual basis.

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 and Compliance team obtains, at a minimum, the current compliance reporting of each vendor (e.g., SOC 2 report, ISO 27001 certificate) and evaluates the results included in the report to determine if controls are sufficient to achieve Atlassian's principal service commitments and system requirements. Any exceptions are assessed to determine the potential impact to the Atlassian control environment.

Section IV: Attachment B – Principal Service Commitments and System Requirement

ATLASSIAN

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

Attachment B - 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.