Atlassian PTY Ltd.

System and Organization Controls (SOC) 3 Report

Report on Jira and Confluence Cloud

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

For the period November 1, 2018 through October 31, 2019

DocuSign Envelope ID: 55377F0E-18A8-4BC6-BBFF-F7856E290251

Management's Report of its Assertions on the Effectiveness of Its Controls over the Jira and Confluence Cloud System Based on the Trust Services Criteria for Security, Availability, and Confidentiality

We, as management of, Atlassian are responsible for:

- Identifying the Jira and Confluence Cloud System (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 Jira and Confluence Cloud System (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, 2018 to October 31, 2019, 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. The organization providing physical safeguards, environmental safeguards, infrastructure support and management, and storage services is referred to as "Sub-service Organizations". The Description (Attachment A) includes only the controls of Atlassian and excludes controls of the sub-service organization. The Description also indicates that certain trust services criteria specified therein can be met only if sub-service organizations' controls assumed in the design of Atlassian's controls are suitably designed and operating effectively along with the related controls at the Service Organization. The Description does not extend to controls of sub-service organizations.

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 us from achieving its specified service commitments.

Very truly yours,

DocuSigned by:
Erika Fisher
8A8D3A5B24B14CD...

Erika Fisher
Chief Legal Officer, Atlassian

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

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

Building a better working world

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 Jira and Confluence Cloud System Based on the Trust Services Criteria for Security, Availability, and Confidentiality (Assertion), that Atlassian Pty Ltd.'s ("Atlassian") controls over the Jira and Confluence Cloud (System) were effective throughout the period November 1, 2018 to October 31, 2019, 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" or "subservice organization") to provide physical safeguards, environmental safeguards, infrastructure support and management, and storage services. The Description of the boundaries of the System (Attachment A) indicates that Atlassian's controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if AWS' 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. Our examination did not extend to the services provided by AWS, and we have not evaluated whether the controls management assumes have been implemented at AWS have been implemented or whether such controls were suitably designed and operating effectively throughout the period November 1, 2018 to October 31, 2019.

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 Jira and Confluence Cloud 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 its principal service commitments and service requirements that are the objectives of our system

A member firm of Ernst & Young Global Limited

- Identifying, designing, implementing, operating, and monitoring effective controls over the Jira and Confluence Cloud 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's assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security, availability, and

A member firm of Ernst & Young Global Limited

Building a better working world

confidentiality, if the subservice organizations applied the controls assumed in the design of Atlassian's controls throughout the period November 1, 2018 to October 31, 2019.

Ernst & Young LLP

Ernst & Young LLP
Irvine, California
January 8, 2020

A member firm of Ernst & Young Global Limited

Attachment A – Atlassian Service Organization's Description of the Boundaries of Its Jira and Confluence Cloud

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 in San Francisco and Mountain View, California, New York City, New York, Sydney, Australia, Manila, Philippines, Yokohama, Japan, Amsterdam, Netherlands, Austin, Texas, Boston, Massachusetts, Falls Church, Virginia, Ankara, Turkey, and Bengaluru, India.

Atlassian's mission is to unleash the potential in every team. Its collaboration software helps teams organize, discuss and complete shared work. Teams of more than 65,000 staff, as well as large and small organizations use Atlassian's project tracking, content creation and sharing, real-time communication, and service management products to work better together and deliver quality results on time. Atlassian products include Jira Software, Jira Service Desk, Confluence, Bitbucket, Statuspage, Trello, and Opsgenie.

The systems in-scope for this report are the Jira and Confluence Cloud systems hosted at Amazon Web Services ("AWS") and the supporting IT infrastructure and business processes, excluding add-ons. This report does not include customer on-premises versions of Jira and Confluence or past Jira and Confluence hosted cloud environments.

Overview of Products and Service

Atlassian's Jira and Confluence Cloud offers several of Atlassian's products as Software as a Service ("SaaS") solution: Jira Suite (Jira Service Desk as the ticketing system and Jira Software as the software), and Confluence. The Jira family of products are used to manage projects and track issues. Confluence offers document management and collaboration.

Infrastructure

Jira and Confluence Cloud are hosted at Amazon Web Services ("AWS") data centers, using the AWS infrastructure as a service offering. The various services making up the runtime and provisioning systems for Jira and Confluence Cloud are deployed in multiple AWS regions across the world (specifically us-east-1, us-west-1, us-west-2, eu-west-1).

Request flow

A typical HTTP request to the Jira or Confluence Cloud applications connect 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 Jira or Confluence Cloud needs are to be routed to. It then forwards the request to the appropriate application cluster. The application, Jira or Confluence Cloud, also contacts 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 Jira and Confluence Cloud APIs via the same path as the other HTTP requests.

Other flow

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 HTTP response to the user such as sending email or running a scheduled job).

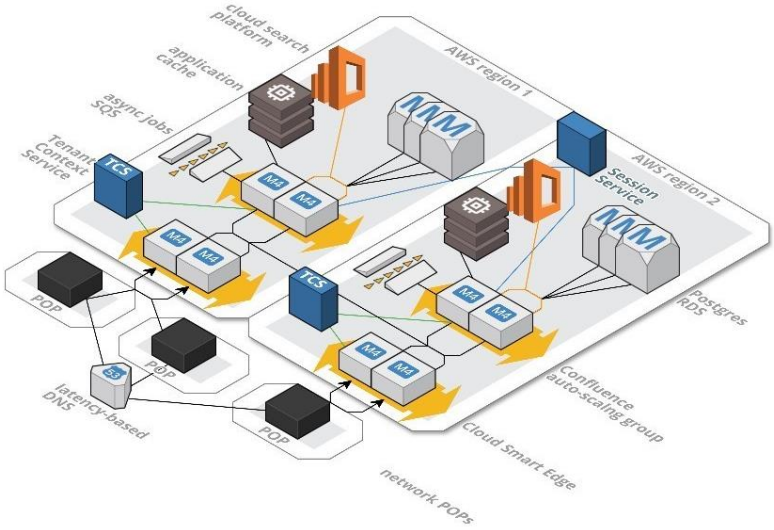

Figure 1: Confluence Architecture Diagram

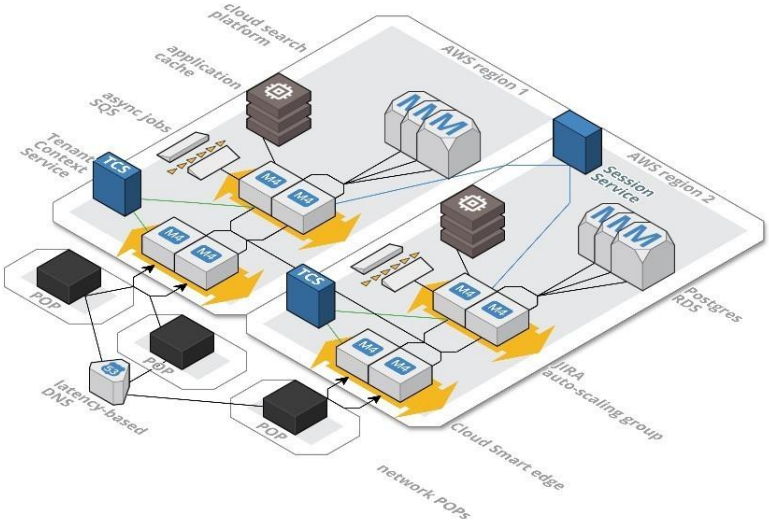

Figure 2: Jira Architecture Diagram

The difference between the Jira and Confluence Cloud architecture is the presence of the cloud search platform which is used by Confluence to provide a searchable text index into all the content.

Network

All network access to Jira and Confluence 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, i.e., it will return a set of IP addresses which are closest to the requestor based on latency. Atlassian has several public ingress end points, each hosted in one of Atlassian's network points of presence ("POP"). These traffic manager clusters terminate public TLS and forward the request to proxies hosted in AWS regions, closest to the data center. 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 Virtual Public Cloud ("VPC"), and all traffic between POPs and AWS regions, as well as between AWS regions, uses the Atlassian shared core network infrastructure, which consists of private dedicated links, which are leased from Tier-1 ISP providers.

Servers

AWS provides infrastructure as a service ("IaaS"). Jira and Confluence have separate AWS accounts for its development and production environments.

Database

Both Jira and Confluence Cloud use logically separate relational databases for each product instance, i.e., tenant data is separated at the database level. Multiple databases may share the same database server that is hosted by AWS. Each database server has an independent synchronous replica in a different availability zone within the same AWS region to mitigate the risk of data lost 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 Jira or Confluence Cloud are stored in the document storage platform (Media Platform). The data in this platform is stored in Amazon S3 to increase 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 the attachment stored in Amazon S3.

Provisioning Architecture

To provision and de-provision products for customers, Atlassian runs a set of systems, each with their own responsibility area. The customer interacts with the provisioning systems through 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 Jira and/or Confluence Cloud. 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 configuration is saved to the Catalogue Service. The Catalogue service then forwards copies of the record to the Tenant Context Service ("TCS"), which then makes the configuration data available to the runtime environment.

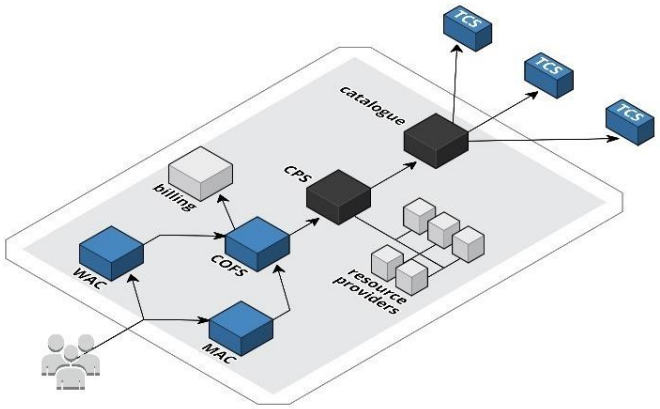

Figure 3: Provisioning Architecture

Software

The following software, services and tools support Jira and Confluence's Cloud control environment:

- www.atlassian.com ("WAC") - Where customers order products, and the shopping cart is hosted
- my.atlassian.com ("MAC") - Where customers manage their current products
- AWS Glacier - data archiving and long-term backup storage service
- AWS Cloudwatch – Monitoring of availability tool
- Alfred – AWS account management tool managed by Atlassian
- Bitbucket Cloud — Atlassian's developed source code and development projects tool
- Confluence - System used for documentation about process and services
- Centrify — Single sign on service used for Atlassian
- Catalogue Service and Catalogue Data Search Service ("CS" and "CDSS") - Administrative store for the configuration of a product and customer
- Cloud Order Fulfilment service ("COFS") - Manages the customer orders and integrates with the billing and invoicing systems
- Cloud Provisioning Service ("CPS") - Manages the services needed to provide a product to a customer. The CPS contacts each part of the system to allocate the needed resources for a product instance, and helps ensure that all these resource allocations complete correctly and in the right order.
- Cloud Search Platform ("CSP") - The search engine for Confluence Cloud (based on Elastic Search)

- Datadog – Monitoring tool
- Deployment bamboo — Atlassian developed continuous integration tool used to perform automated testing and deployment activities
- GoogleAuth — Single sign on service used for Atlassian employees and contractors
- Hosted Account Management System ("HAMS") – Primary customer data process that is responsible for the core purchasing and billing functions
- Identity services - Management of users, authentication and authorization
- Jira — Ticketing system used for incident management, user access provisioning, and change management process
- Lever — Hiring tool
- Media Platform (document store) - Stores attachments for Jira and Confluence Cloud, using Amazon S3
- Monarch (database manager) - Manages the per-customer databases for the products, using AWS RDS
- Nexpose — Vulnerability scanning tool
- Pollinator – Monitoring of security and availability tool
- Pagerduty – Alerting tool for monitoring of availability
- SignalFX — Atlassian's 3rd party vendor used for system monitoring and alerting platform
- Slack — Collaboration or instant messaging tool
- Sourceclear - Software tool to identify vulnerabilities in 3rd-party libraries used by application code
- Tenant Catalogue Service ("TCS") - Stores the product-specific configuration for a customer for consumption at runtime
- Workday — Human Resource (HR) system; including performance feedback

AWS is a third-party vendor. Atlassian performs a review of the SOC 2 report of the third-party vendor. The evaluation of the SOC report is performed and reviewed by the Risk and Compliance Team, which includes an assessment of the complimentary user entity control, subservice organizations, and mapping of the controls to key risks. If there are exceptions, Atlassian will review the severity and impact of the exceptions, and if needed, follow up with the vendor. Centrify, GoogleAuth, Datadog, Lever, Nexpose, Pagerduty, Pollinator, SignalFX, Slack, Sourceclear, and Workday are third-party vendors; however, customer data is not stored in these applications. These are supporting and monitoring tools, and are only applicable to support certain controls and criteria.

WAC, MAC, Bitbucket Cloud, Confluence, CS, CDSS, COFS, CPS, CSP, Deployment bamboo, HAMS, Identity services and Jira are Atlassian managed tools and are in-scope in the controls discussed below.

Vendor agreements, including any security, availability, and confidentiality commitments, are reviewed by appropriate Atlassian management during the procurement process. Prior to services rendered, the vendor and Atlassian are required to sign the vendor agreement terms and conditions.

Data

Customers sign up for Jira and/or Confluence Cloud on www.atlassian.com. Upon accepting the terms and conditions, and completing the sign-up process, dedicated product databases are created in the AWS Postgres RDS clusters, which are logically separated from other customers' data, using both a separate database and separate credentials. Once complete, the customer can start using Jira and/or Confluence Cloud. Metadata information about the customer is also written into the Catalogue Service ("CS") database which stores the master copy of the customers' configuration. 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.

Production customer data is encrypted in transit within Atlassian's network, which is managed by AWS. Effective June 2019, Atlassian implemented data encryption at rest for production customer data. AWS' SOC 2 report is reviewed at least annually by Atlassian. External users connect to Jira and Confluence Cloud using encryption via the TLS protocol and customer attachments in Jira and Confluence are encrypted in the Media Platform. Additionally, there is no production data residing in the non-production environments.

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:

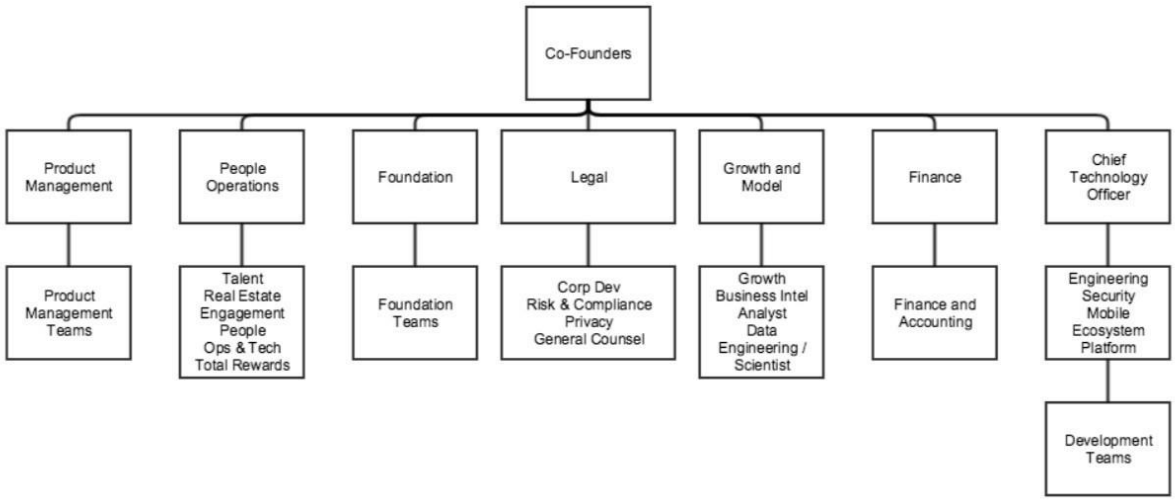

Figure 4: Atlassian's Organizational Chart

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 is available to all Atlassian employees via Atlassian's HR system, Workday.

The Co-Founders are responsible for directing all designated areas including Product Management, People Operations, Foundation, Legal, Growth and Modeling, and the Technology teams. All teams have full responsibility over key operations within Atlassian:

- Product Management — focuses on validating the demands of customers, provides insight and guidance around minimum viable product and user experience.
- People Operations (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 eliminate 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, public relations, risk and compliance.
- Growth and Model — responsible for monitoring business trends, analytics, data engineering and data science.
- Finance — responsible for handling finance and accounting.
- Chief Technology Officer (Technology Operations) — oversees Engineering, Security, Mobile, Ecosystem and Platform.
    - Head of Engineering, Software Teams oversees all operations for the products.
    - Development Manager:
        - Drives and improves product quality and innovation, team productivity, manages simultaneous projects in an agile fashion, customer satisfaction and product supportability.
        - Coordinate multiple streams of software development, involving multiple teams, geographic distribution and indirect reports.
        - Collaborate with Product Management by contributing to roadmaps, setting priorities, and providing estimates.
        - Collaborate with Customer Support to help ensure customer success and drive quality improvements.
        - Promote, define, refine, and enforce best practices and process improvements that fit Atlassian's agile methodology.
        - Provide visibility through metrics and project status reporting.
        - Set objectives for people and teams and holds them accountable.

- Work with Recruitment to attract and hire outstanding individuals to create high performing balanced teams.
- Lead by example and practice an inclusive management style.

Complementary Subservice Organizations Controls

Atlassian uses Amazon Web Services ("AWS" or "subservice organization") to provide physical safeguards, environmental safeguards, infrastructure support and management, and storage services.

The affected criteria are included below along with the expected minimum controls in place at the third parties.

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.	Amazon Web Services (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.	Amazon Web Services (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 management approval. Documented procedures exist for the identification and escalation of potential physical security breaches. Visitors must be signed in by an authorized workforce member before gaining entry and must be escorted at all times.
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.	Amazon Web Services (AWS)	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.	Amazon Web Services (AWS)	Environmental protections have been installed including the following: • Cooling systems • Battery and generator backups • Smoke detection • Dry pipe sprinklers Environmental protection equipment receive maintenance on at least an annual basis.

Management's monitoring control over sub-service providers

Due diligence procedures are in place upon engagement and at least annually for third-party service providers according to the Information Management Standard. The annual evaluation includes an assessment of the sub-service providers related SOC, ISO, Information Security Compliance Policies, response to Security & IT Questionnaire, or other attestation reports, as well as an impact analysis for any identified deficiencies.

Attachment B - Principal Service Commitments and System Requirements

Atlassian designs its processes and procedures to meet the objectives of related to the Jira and Confluence Cloud system. Those objectives are based on the service commitments that Atlassian makes to user entities, the laws and regulations that govern the provision of Jira and Confluence Cloud system and the financial, operational, and compliance requirements that Atlassian has established for the system.

Security, availability, and confidentiality commitments to user entities are documented and communicated in the terms of services within the sign-up page in Jira and Confluence Cloud 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 Jira and Confluence Cloud system. Such security and confidentiality controls include permitting and restricting system users to access to 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 implement to keep the Jira and Confluence Cloud system and customer's data safe. This includes the use of encryption technologies to protect customer data at rest and in transit, and formal process 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 process to detect security and vulnerability issue, 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 Jira and Confluence Cloud system.