Atlassian PTY Ltd.

System and Organization Controls (SOC) 3 Report

Report on Jira Service Management

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

For the period November 1, 2019 through October 31, 2020

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

We, as management of, Atlassian are responsible for:

- Identifying the Jira Service Management (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, 2019 to October 31, 2020, 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 System (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:
Stan Shepard
B29BD040945A4FC...

Stan Shepard
Deputy General Counsel, Atlassian

Ernst & Young LLP
18101 Von Karman
Ave #1700
Irvine, CA 92612

Tel: +1 949 794 2300
Fax: +1 866 492 5140
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 Service Management System Based on the Trust Services Criteria for Security, Availability, and Confidentiality (Assertion), that Atlassian's controls over Jira Service Management (System) were effective throughout the period November 1, 2019 to October 31, 2020, 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 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 System 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, 2019 to October 31, 2020.

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

- Identifying the Jira Service Management (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
- 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

Building a better working world

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 aforementioned criteria for security, availability, and confidentiality (applicable trust services criteria), and if the subservice organization applied the controls assumed in the design of Atlassian's controls throughout the period November 1, 2019 to October 31, 2020.

Ernst & Young LLP

January 13, 2021
Irvine, California

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

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), Turkey (Ankara), and India (Bengaluru).

Atlassian's mission is to unleash the potential in every team. Its collaboration software helps teams organize, discuss, and complete shared work. Thousands of teams across large and small organizations worldwide use Atlassian's project tracking, content creation and sharing, real-time communication, and service management products to work better together and deliver quality results on time. Atlassian products include Jira, Jira Service Management, Confluence, Bitbucket, Statuspage, Trello, Opsgenie, Jira Align, and Halp.

The systems in-scope for this report are the Jira Service Management system hosted at Amazon Web Services ("AWS") and the supporting IT infrastructure and business processes, excluding add-ons. This report does not include customer on-premise versions of Jira Service Management.

Overview of Products and Service

Jira Service Management 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.

Jira Service Management includes the power of Opsgenie - a major incident management platform for operating always-on services that empowers Dev and Ops 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 them to collaborate and take rapid action.

Infrastructure

Infrastructure is managed separately for Jira Service Management and Opsgenie internally.

Jira Service Management:

Jira Service Management is 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 Service Management are deployed in multiple AWS regions across the world (specifically us-east-1, us-west-2, eu-central-1, eu-west-1, ap-southeast-1, ap-southeast-2).

A typical request to the Jira Service Management application 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 Jira Service Management needs are to be routed to. It then forwards the request to the appropriate application cluster. The application, Jira Service Management, 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 Service Management APIs via the same path as the other 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 response to the user such as sending email or running a scheduled job).

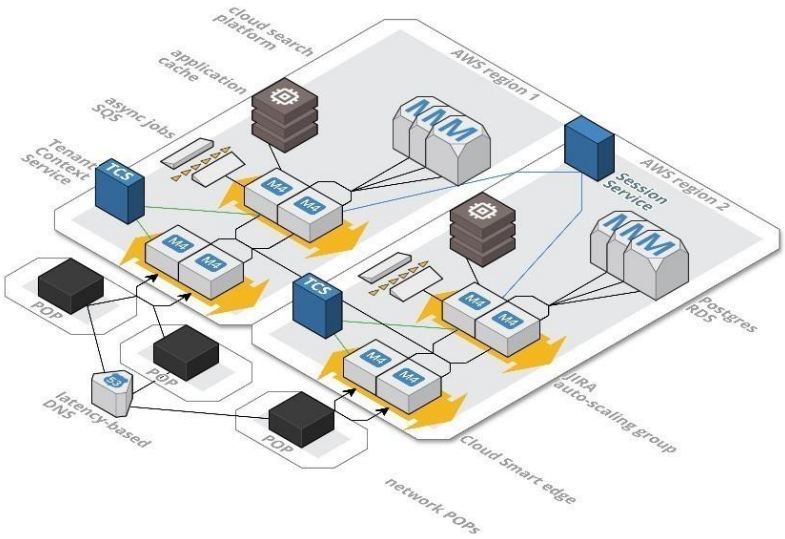

Figure 1: Jira Architecture Diagram

Opsgenie:

Opsgenie is hosted at Amazon Web Services ("AWS") data centers, US-West (Oregon) and US-East (Ohio), and EU (Frankfurt) and EU (Ireland), using the AWS Infrastructure as a Service offering ("IaaS"). However, all Jira Service Management Opsgenie data is stored in the US by default. The services that make up the Opsgenie system are primarily isolated within multiple private networks, which is spread out to multiple data centers and regions for redundancy, high availability, and fault-tolerance.

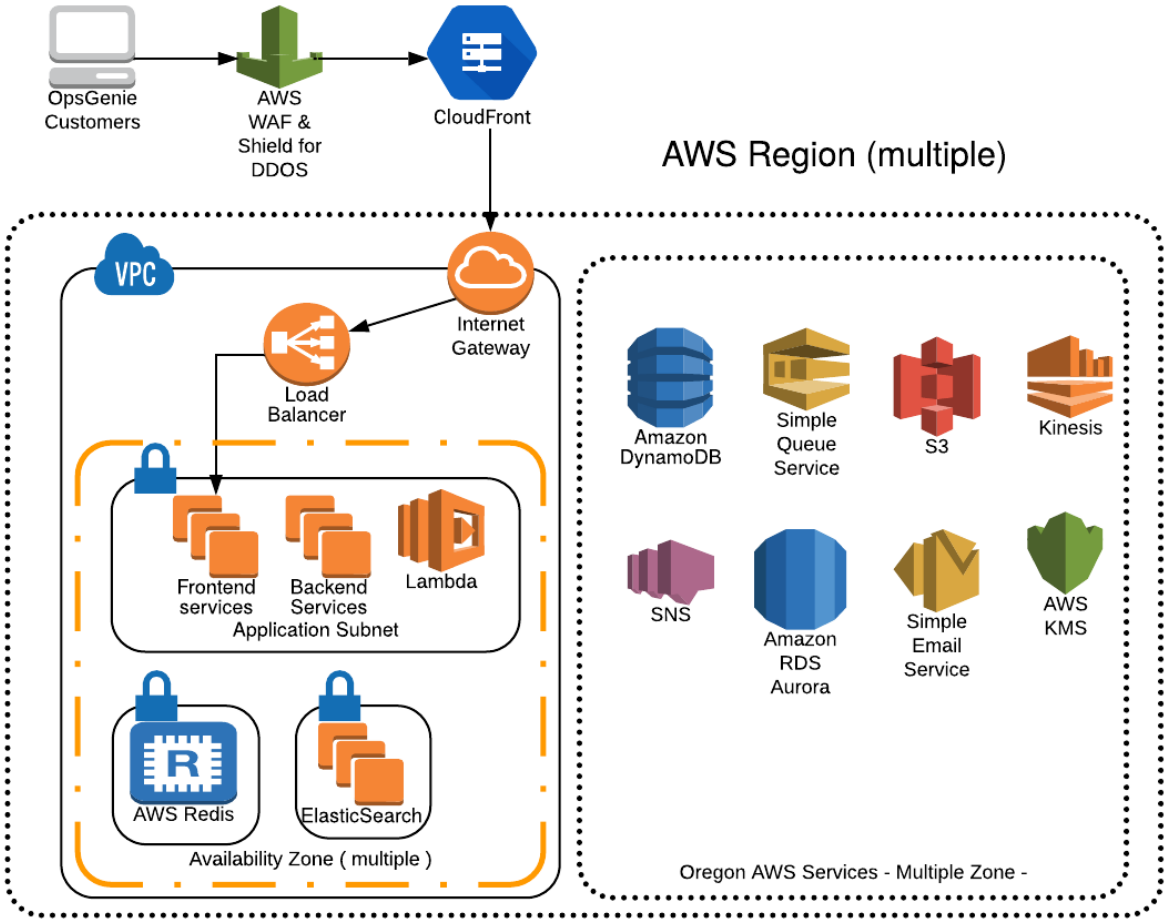

Figure 2: Opsgenie's Infrastructure

The core Opsgenie application is composed of the following AWS services within Atlassian's network:

- **AWS WAF and Shield, CloudFront and Load Balancers:** These services are used as a proxy to forward public traffic to Opsgenie local network ("Opsgenie origin"), with over 200 AWS Points of Presence ("POP") locations. AWS CloudFront offers DDOS and security protection and fast access to Opsgenie origin. AWS CloudFront forwards traffic to public facing AWS Load Balancers and the AWS load balancers forward traffic to AWS EC2 based applications within private networks (AWS VPC). AWS VPC Access Control Lists and AWS EC2 Security groups provide additional network segmentation and firewall layers.
- **AWS Simple Queue Service, Kinesis, and SNS:** These are messaging queue and delivery services that AWS manages for communication and asynchronous event processing.
- **ElasticSearch:** Amazon Elasticsearch service used for indexing data for the purposes of search.

- **Redis:** Used for data caching for the frequently accessed configuration data on DynamoDB.
- **AWS DynamoDB and S3:** Used for storing customer data.
- **AWS RDS Aurora and MySQL:** Reporting service to help run custom reports.
- **AWS Key Management Service ("KMS"):** AWS service that provides encryption at rest (AES-256 key encryption).

Servers

AWS provides Infrastructure-as-a-Service ("IaaS") which runs Jira Service Management. However, the virtual server and operating system configurations are managed by Atlassian. The AWS IaaS for Jira Service Management spans multiple data centers and regions. Jira Service Management has separate AWS accounts for its development and production environments.

Database

Databases are managed separately for Jira Service Management and Opsgenie internally.

Jira Service Management:

Jira Service Management uses logically separate AWS RDS 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 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 Jira Service Management 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.

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.

Jira Service Management uses 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 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 Jira Service Management 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.

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 Amazon DynamoDB 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.

The data in all of the above cases is encrypted at rest.

Software

The following software, services, and tools support the control environment of Jira Service Management:

Component	Description
Hosting Systems	• Amazon EC2
Storage and Database	• Amazon Relational Database Service (RDS) • Amazon DynamoDB • Amazon Simple Storage Service (S3)
Network	• Amazon Virtual Private Cloud • Amazon Load Balancers • Amazon CloudFront • Amazon Web Application Firewall (WAF) • Corporate firewall
Build, Release, and Continuous Integration Systems	• Bitbucket • Bamboo • Internal CI/CD tool • Jenkins
Access Management	• Active Directory • Idaptive (Single Sign On) • Duo (Two-factor authentication)
Monitoring and Alerting	• Splunk • SignalFX • NewRelic • Opsgenie
Vulnerability Scanning	• Nexpose • Cloud Conformity • SourceClear
Human Resource	• Workday

	• Lever
Notifications	• Nexmo • Mailgun • Twilio • Pubnub

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

Data

Customers sign up for Jira Service Management on https://www.atlassian.com. Upon accepting the terms and conditions, and completing the sign-up flow, a new database record and unique identifier are created in the database 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.

Additionally, there is no production data residing in the non-production environments and complies with the confidentiality requirements based on the region in which customers select.

Customer data is encrypted at rest and external connections to Jira Service Management are encrypted in transit via the TLS protocol. Customer data is only stored in production environments and is not transferred to any non-production environment. Additionally, connections within the Atlassian production environment are also encrypted in transit to further protect customer data.

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:

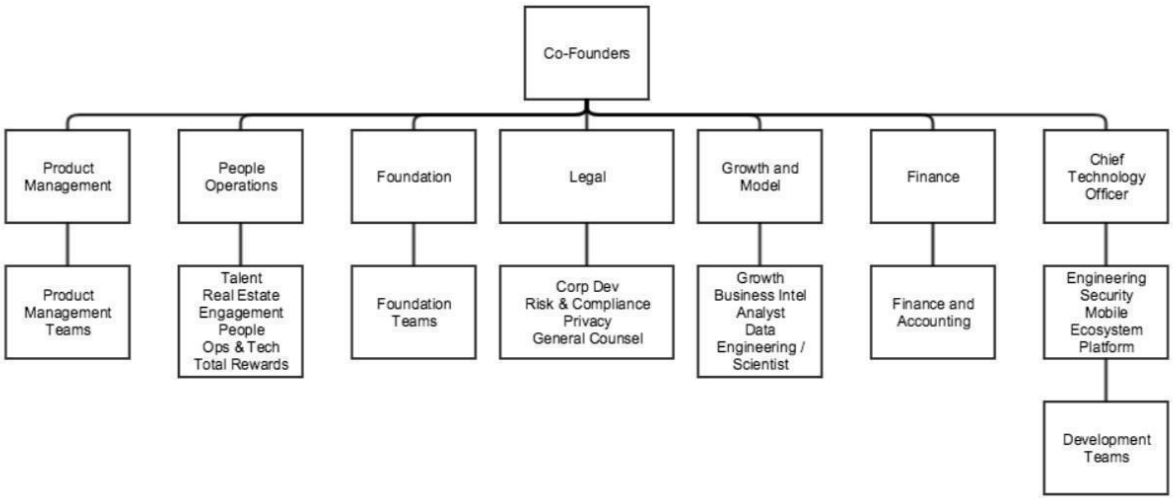

Figure 3: Atlassian's Organizational Chart

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 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 maintain 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 hold 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 utilizes subservice organizations to perform certain functions as described in the description above. Rather than duplicate the control tests, controls at Amazon Web Services are not included in the scope of this report. The affected criteria are included below along with the expected controls of Amazon Web Services ("AWS").

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 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.
CC8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data,	Amazon Web Services (AWS)	Changes are authorized, tested, and approved prior to implementation.

Criteria	Service Organization	Controls
software, and procedures to meet its objectives.		
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 is monitored for incidents or events that impact AWS assets.

Management's Monitoring Control over the Subservice 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 related to the Jira Service Management 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 Service Management 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 Service Management 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 Service Management system. 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 Jira Service Management system 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 Jira Service Management system.