Atlassian PTY Ltd.

System and Organization Controls (SOC) 3 Report

Report on Jira Align

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's Jira Align

SECTION I: ATLASSIAN'S MANAGEMENT ASSERTION

Management's Report of Its Assertions on the Effectiveness of Its Controls Over the Jira Align 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 Jira Align (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") and Microsoft Azure ("Azure") 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 AWS and Azure. The Description also indicates that certain trust services criteria specified therein can be met only if AWS and Azure's controls assumed in the design of Atlassian's controls are suitably designed and operating effectively along with the related controls at AWS and Azure. The Description does not extend to controls of AWS and Azure.

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

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

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 Align System Based on the Trust Services Criteria for Security, Availability, and Confidentiality (Assertion), that Atlassian's controls over the Jira Align (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 uses Amazon Web Services ("AWS") and Microsoft Azure ("Azure") 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 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 Azure's 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 Azure. Our examination did not extend to the services provided by AWS and Azure, and we have not evaluated whether the controls management assumes have been implemented at AWS and Azure 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 Jira Align (System) and describing the boundaries of the System
- Identifying the 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 the 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 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. 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 Align System hosted at Amazon Web Services ("AWS"), the Business Intelligence Enterprise Insights reporting system ("Enterprise Insights") hosted at Microsoft Azure, and the supporting IT infrastructure and business processes.

Overview of Products and Service

Jira Align is a scaled agile management system that leverages Agile at Scale frameworks such as the Scaled Agile Framework ("SAFe") to provide visibility, coordination, and management at program, portfolio, and enterprise levels. Jira Align provides services to customers globally, primarily in the technology industry. Jira Align simplifies software at scale by bringing the business and software development organizations together on one intuitive platform.

Jira Align bi-directionally integrates with third-party systems at the team level, enabling coordination between product owners, scrum masters, program managers, and release train engineers. The application provides a real-time visualization of the work being performed across users. Organizations use Jira Align to scale above the individual team level and support strategic decision making, such as development capacity optimization and investment decisions.

Jira Align can perform the following key functions based on customer configuration:

- Track financials, resource allocation, and progress across strategies
- Map strategy to execution and model work up to the executive level
- Report on investment performance and plan delivery
- Leverage value streams to minimize bottlenecks and optimize value throughput

- Make work visible in real-time across all teams, products, and programs
- Create one centralized place to optimize end-to-end strategic operations

Infrastructure

The Jira Align Software-as-a-Service ("SaaS") production environment runs on Microsoft Windows and Microsoft SQL servers in Amazon Web Services ("AWS"). The Company uses Microsoft Azure cloud hosted environment to support the data warehouse for their business intelligence ("BI") product, Enterprise Insights. AWS and Azure are responsible for maintaining the security of production infrastructure in their cloud hosted environments.

Customers may choose where they'd like their data hosted upon sign-up. The options are: AWS US-East-2, AWS AP-Southeast-2, AWS EU-Central-1, Azure East US, and Azure West Europe.

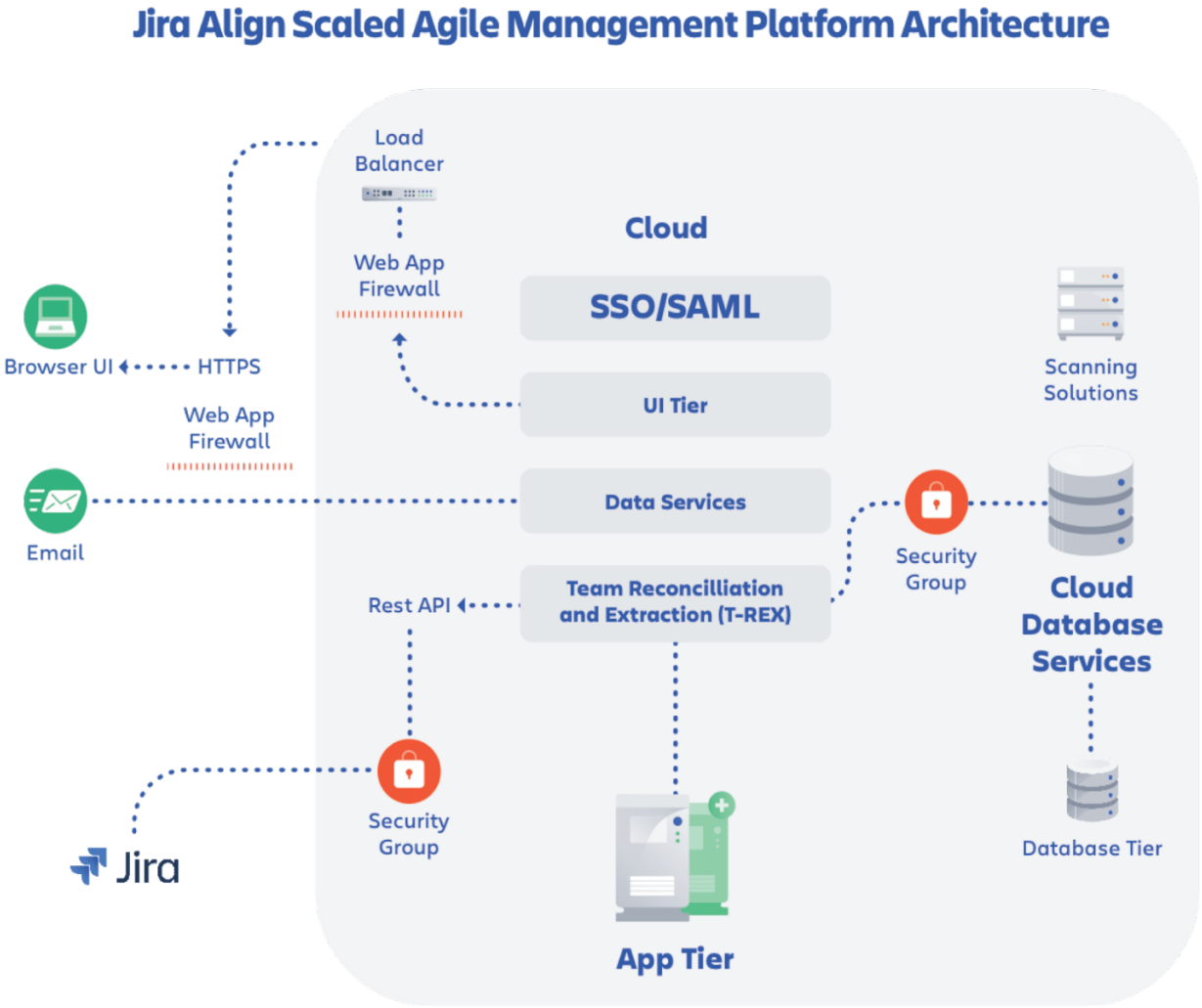

Figure 1: Jira Align Infrastructure

Jira Align is a Microsoft Windows web application developed, maintained, and enhanced by Atlassian. Each Jira Align customer is supplied with a unique external website and web interface supported by the platform. The web interface is a multi-user application that

customers use to create and manage work items and tasks to support the execution of their projects and work streams. Organizations can formulate, document, and track strategic plans through execution. The web interface also provides reporting capabilities that can be used to generate reports by person, work, time, product, customer, and value.

Customers can also use Jira Align to configure email notifications and updates to work items that are integrated from other team tools such as Jira, Azure DevOps, Trello, and Rally. The Connector provides customers the ability to bi-directionally integrate data from one or more team tools into Jira Align for consolidated reporting.

Enterprise Insights is a Business Intelligence ("BI") data warehouse that is offered as an add-on product for existing customers. Customers can use Enterprise Insights to create custom reports that combine their Jira Align data with data from other systems of record to fulfill the unique reporting needs of their users. Customers are responsible for the completeness and accuracy of the data input to Enterprise Insights, and data output of reports from Enterprise Insights.

The processes and controls managed by AWS and Microsoft Azure are excluded from the scope of this report.

Servers

AWS provides Infrastructure as a Service ("IaaS") and is managed by Atlassian. The network, IAM roles, key management, Active Directory, database administration, patching, and tier-1 operational support are managed by the Jira Align SRE team. The operating system images are provided by AWS and the required software components are defined by the Jira Align team.

Microsoft Azure provides Platform as a Service ("PaaS") / Software as a Service ("SaaS") with respect to the Enterprise Insights BI solution.

Database

The primary datastore for Jira Align is Microsoft SQL Server RDS, which is hosted in AWS. The RDS cluster includes a leader and multiple followers, and its nodes are spread out across at least 2 Availability Zones for fault-tolerance and redundancy. The data is encrypted at rest via 256-bit Advanced Encryption Standard (AES-256) on Elastic Block Storage. The keys are managed via AWS Key Management System ("KMS"), with access rights designated to a separate IAM role.

Note that all data is stored in SQL server including search indexes and user attachments.

The primary datastore for Enterprise Insights BI is generated hourly by an ETL job running within the AWS Virtual Private Cloud. This datastore is hosted in Microsoft Azure. The data warehouse is encrypted via Azure encryption at rest.

Software

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

Component	Description
Hosting Systems	● Amazon EC2
Storage and Database	● Amazon Relational Database Service (RDS) ● Microsoft Azure Database
Network	● Amazon Virtual Private Cloud ● Amazon Load Balancers ● Corporate firewall
Build, Release, and Continuous Integration Systems	● Bitbucket ● AppVeyor ● Testery ● Octopus
Access Management	● Active Directory ● Idaptive (Single Sign On) ● Duo (Two-factor authentication)
Monitoring and Alerting	● Alert Logic ● Splunk ● SignalFX ● Opsgenie
Vulnerability Scanning	● Nexpose ● Cloud Conformity SourceClear
Human Resource	● Workday ● Lever

Amazon Web Services ("AWS") and Microsoft Azure ("Azure") are third-party vendors that provide physical safeguards, environmental safeguards, infrastructure support and

management, and storage services. Atlassian has identified the complementary subservice organization controls of AWS and Azure 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 can sign up for Jira Align through a request form using https://atlassian.com/software/jira/align#contact. Upon request, a designated customer support member will discuss various components of the customer's infrastructure to understand how the customer's platform should be designed and implemented, and a customer Master Service Agreement ("MSA"), which includes any specific terms and conditions between the two parties, is outlined. Once the customer acknowledges the terms and conditions either through the Atlassian website or through the signed customer MSA, the customer's account and environment will be created. An account cannot be made for any of Atlassian's products without first being directed to acknowledge the Cloud Terms of Service.

Customer data is exclusively restricted to the AWS and Azure hosted environments. It is not maintained in hard copy nor local electronic copy by Atlassian. Customer data is collected by manually entering project and program customer file uploads. Customer data are replicated via two-way synchronization. Customers communicate with Jira Align Solution Architecture and Support teams as part of the implementation process. Customers enter data and upload files through the website to communicate their current process and end goals for an implementation. All files are stored on SQL servers hosted by AWS.

Customer data is also segmented by separate databases dedicated to each customer via both multi-tenant and dedicated virtual private clouds ("VPCs") on Amazon Web Services ("AWS").The multi-tenant VPCs each have a unique user account and connection string which separate each Jira Align customer's data on the database service into separate databases. Meanwhile, dedicated VPCs are created for requesting customers, whereby the VPC network is not shared with other customers, thus, inherently having a dedicated RDS database instance.

Customer data is restricted to the production environment and does not reside in any non-production or development environments. Additionally, all customer data in the production environment is protected in alignment with Atlassian's System Acquisition, Development, and Maintenance Policy.

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:

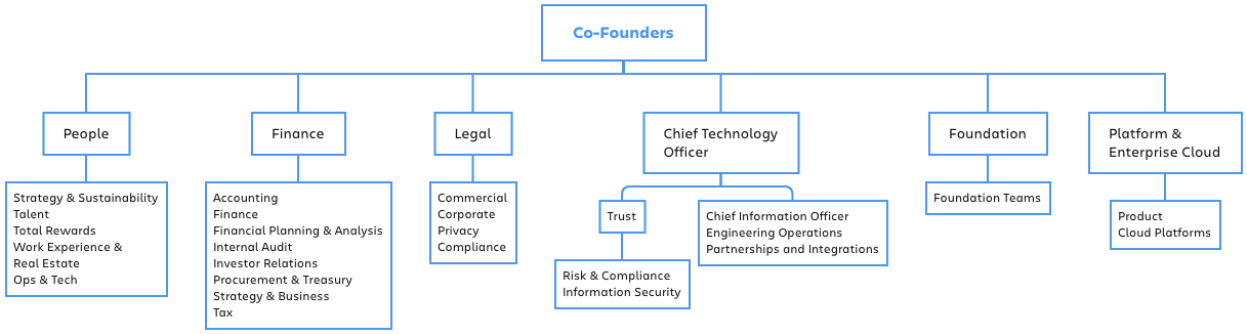

Figure 2: Atlassian's Organizational Chart

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 Amazon Web Services and Microsoft Azure 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") or Microsoft Azure ("Azure").

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, Azure	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 and Microsoft Azure.
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.

Criteria	Service Organization	Controls
	Azure	Procedures have been established to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors. Security verification and check-in are required for personnel requiring temporary access to the interior datacenter facility including tour groups or visitors. Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team. Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals. The datacenter facility is monitored 24x7 by security personnel.
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, Azure	Changes are authorized, tested, and approved prior to implementation.
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, Azure	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

Criteria	Service Organization	Controls
		that impact AWS assets.

Vendor Management

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

As part of the onboarding process, high-risk vendors are subject to a risk assessment and detailed review by internal Atlassian cross-functional subject matters experts ("SMEs"). This involves evaluating the supplier's control environment and overall security posture based on information contained in supplier questionnaires, compliance reporting (e.g., SOC2), and policies. Vendor agreements, including terms and conditions, any security, confidentiality, and availability related commitments, are also reviewed and signed prior to engaging with any vendor.

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

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

SECTION IV: ATTACHMENT B – PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Attachment B - Principal Service Commitments and System Requirements

Atlassian designs its processes and procedures to meet the objectives of the Jira Align system. Those objectives are based on the service commitments that Atlassian makes to user entities, the laws and regulations that govern the provision of the Jira Align 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 Align 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 Align 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 Align 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 Align system.