KPMG Assurance and Consulting Services LLP
Embassy Golf Links Business Park,
Pebble Beach, B Block, 1st and 2nd Floor,
Off Intermediate Ring Road,
Bengaluru 560 071 India
Tel: +91 80 6833 5000
Fax: +91 80 6833 6999

Atlassian India LLP
3rd floor, Sunriver, 11/1,12/1, Embassy Golf Links Business Park, Bengaluru, Karnataka, India – 560071

30 April 2025

Attention: Ashish Suri, Head of Governance, Risk and Compliance.

KPMG Assurance and Consulting Services LLP (hereinafter referred to as "KPMG", "We", "Our") have completed SOC 2 Type 1 examination for Atlassian Corporation Limited, Atlassian Australia 1 Pyt Limited, and Atlassian India LLP (herein after referred to as "Atlassian", "service organization", "you") as outlined in our engagement letter. This report to you represents our final SOC 2 Type 1 report.

The data included in this report was obtained from you, on 28 February 2025. We have no obligation to update our report or to revise the information contained therein to reflect events and transactions occurring subsequent to 28 February 2025. The attached report is the electronic version of our signed deliverable, which has been issued to you in the hard copy format.

This report sets forth our views based on the completeness and accuracy of the facts stated to KPMG and any assumptions that were included. If any of the facts and assumptions is not complete or accurate, it is imperative that we be informed accordingly, as the inaccuracy or incompleteness thereof could have a material effect on our conclusions.

While performing the work, we assumed the genuineness of all signatures and the authenticity of all original documents. We have not independently verified the correctness or authenticity of the same.

This report is intended solely for the information and use of the management of Atlassian, its user entities and the independent auditors of user entities (collectively referred to as authorized parties) and is not intended to be, and should not be, used by anyone other than these authorized parties. If this report is received by anyone other than authorized parties, the recipient is placed on notice that the attached SOC 2 Type 1 report has been prepared solely for authorized parties for their internal use and this report and its contents shall not be shared with or disclosed to anyone by the recipient without the express written consent of Atlassian and KPMG. KPMG shall have no liability and shall pursue all available legal and equitable remedies against recipient, for the unauthorized use or distribution of this report. We have been engaged by Atlassian for the Services and to the fullest extent permitted by law, we will not accept responsibility or liability to any other party in respect of our Services or the report. We thus disclaim all responsibility or liability for any costs, damages, losses, liabilities, expenses incurred by such other party arising out of or in connection with the report or any part thereof. By reading our report the reader of the report shall be deemed to have accepted the terms mentioned hereinabove.

Please contact us if you have any questions or comments. We look forward to providing services to your company.

Yours sincerely,

M N Gururaja

Partner, KPMG Assurance and Consulting Services LLP

SYSTEM AND ORGANIZATION CONTROLS (SOC 2) TYPE 1 REPORT

Report on description of systems for providing Atlassian Focus, a product of Atlassian, and on the suitability of design of its controls relevant to the Security, Availability, and Confidentiality as of 28 February 2025.

TABLE OF CONTENTS

INDEPENDENT SERVICE AUDITOR'S ASSURANCE REPORT 4

STATEMENT BY THE SERVICE ORGANIZATION 8

SERVICE ORGANIZATION'S DESCRIPTION OF THE SYSTEM 10

INTRODUCTION 11
SCOPE OF THE REPORT 11
OVERVIEW OF SERVICE ORGANIZATION 11
SERVICES PROVIDED BY SERVICE ORGANIZATION TO USER ENTITIES 11
SUB SERVICE ORGANIZATION 12
SYSTEM OVERVIEW 12
COSO FRAMEWORK 12
PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS 14
COMPONENTS OF THE SYSTEM 14
INFRASTRUCTURE 14
NETWORK 14
DATA 15
SOFTWARE 15
PEOPLE 17
PROCESSES AND PROCEDURES 18
POLICY REQUIREMENTS 19
POLICY REVIEW PROCESS 19
DATA CLASSIFICATION AND CONFIDENTIALITY OF INFORMATION 19
CONTROL ENVIRONMENT 20
INFORMATION AND COMMUNICATION 21
RISK ASSESSMENT AND MITIGATION 22
MONITORING 22
CONTROL ACTIVITIES 23
AVAILABILITY 24
CONFIDENTIALITY 24
COMPLEMENTARY USER ENTITY CONTROLS 25
COMPLEMENTARY SUB-SERVICE ORGANIZATION CONTROLS 26
MAPPING OF SOC2 TRUST SERVICES CRITERIA WITH CONTROL ACTIVITIES 28
ANNEXURE: LIST OF ABBREVIATIONS: 63

SECTION 1

INDEPENDENT SERVICE AUDITOR'S ASSURANCE REPORT

KPMG Assurance and Consulting Services LLP
Embassy Golf Links Business Park,
Pebble Beach, B Block, 1st and 2nd Floor,
Off Intermediate Ring Road,
Bengaluru 560 071 India
Tel: +91 80 6833 5000
Fax: +91 80 6833 6999

INDEPENDENT SERVICE AUDITOR'S ASSURANCE REPORT

To
The Management,
Atlassian India LLP

Scope

We have been engaged to report on Atlassian Corporation Limited, Atlassian Australia 1 Pyt Limited, and Atlassian India LLP Service Organization's (hereinafter referred to as "Atlassian" or "service organization") accompanying description of its system in section 3 of Atlassian Focus product as of 28 February 2025 (the description), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report,* in AICPA Description Criteria, (the description criteria), and the suitability of the design of controls stated in the description as of 28 February 2025 to provide reasonable assurance that Atlassian's service commitments and system requirements would be achieved based on the trust services criteria, if its controls operated effectively, relevant to security, availability, and confidentiality, (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy in AICPA Trust Services Criteria.*

Atlassian uses AWS as subservice organizations to provide infrastructure support services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Atlassian, to achieve Atlassian's service commitments and system requirements based on the applicable trust services criteria. The description presents Atlassian's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Atlassian's controls. The description does not disclose the actual controls at the subservice organization. Our engagement did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Atlassian, to achieve Atlassian's service commitments and system requirements based on the applicable trust services criteria. The description presents Atlassian's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Atlassian's controls. Our engagement did not include such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

Atlassian is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Atlassian's service commitments and system requirements were achieved. Management of Atlassian has provided the accompanying statement in section 2 (the Management Statement) about the description and the suitability of design of controls stated therein.

Atlassian is also responsible for preparing the description and statement, including the completeness, accuracy, and method of presentation of the description and statement; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of Atlassian's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design of controls stated in the description based on the evidence we have obtained in our engagement.

Our engagement was conducted in accordance with International Standard on Assurance Engagements 3000 (Revised), Assurance Engagements *Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. That standard requires that we plan and perform our engagement to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description cand the controls stated therein were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria, if the service organization's controls operated effectively. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

A reasonable assurance engagement to report on the description of a service organization's system and the suitability of the design of controls involves the following:

- obtaining an understanding of the system and the service organization's service commitments and system requirements;
- assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed;
- performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria;
- performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization would achieve its service commitments and system requirements based on the applicable trust services criteria if those controls operated effectively;
- evaluating the overall presentation of the description; and
- performing such other procedures as we considered necessary in the circumstances.

Service Auditor's Independence and Quality Management

We have complied with the independence and other ethical requirements of the *International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants (including International Independence Standards)* (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

The firm applies International Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements*, which requires the firm to design, implement and operate a system of quality management including documented policies or procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that each individual report user may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the Description and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects,

a) the description presents Atlassian's system that was designed and implemented as of 28 February 2025 in accordance with the description criteria; and

b) the controls stated in the description were suitably designed as of 28 February 2025 to provide reasonable assurance that Atlassian's service commitments and system requirements would be achieved based on the applicable trust services criteria if controls operated effectively as of 28 February 2025, and the subservice organization and user entities applied the complementary controls assumed in the design of Atlassian's controls as of 28 February 2025.

Restricted Use

This report is intended solely for the information and use of Atlassian and user entities of Atlassian's system as of 28 February 2025 who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization;
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties;
- Internal control and its limitations;
- complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements;
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services;
- The applicable trust services criteria; and
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be and should not be used by anyone other than these specified parties.

KPMG Assurance and Consulting Services LLP
30 April 2025

SECTION 2

STATEMENT BY THE SERVICE ORGANIZATION

ASSERTION OF ATLASSIAN MANAGEMENT

We have prepared the accompanying description of Atlassian Corporation Limited, Atlassian Australia 1 Pyt Limited, and Atlassian India LLP Service Organization (hereinafter referred to as "Atlassian" or "service organization") in section 3 of its Atlassian Focus system as of 28 February 2025 (the description), based on the criteria for a description of a service organization's system in DC section 200, 2018 *Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (the *description criteria*). The description is intended to provide report users with information about the Atlassian's system that may be useful when assessing the risks arising from interactions with Atlassian's system, particularly information about system controls that Atlassian has designed implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to *Security, Availability, and Confidentiality,* (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.*

Atlassian uses AWS as subservice organizations to provide infrastructure support services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Atlassian, to achieve Atlassian's service commitments and system requirements based on the applicable trust services criteria. The description presents Atlassian's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Atlassian's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Atlassian, to achieve Atlassian's service commitments and system requirements based on the applicable trust services criteria. The description presents Atlassian's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Atlassian's controls.

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

a) The description presents Atlassian's system that was designed and implemented as of 28 February 2025 in accordance with the description criteria.

b) The controls stated in the description were suitably designed as of 28 February 2025 to provide reasonable assurance that Atlassian's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of 28 February 2025 and if subservice organization and user entities applied the complementary controls assumed in the design of Atlassian's controls as of that date.

SECTION 3

SERVICE ORGANIZATION'S DESCRIPTION OF THE SYSTEM

Introduction

Scope of the Report

The scope of the report includes the description of Atlassian Corporation Limited, Atlassian Australia 1 Pyt Limited, and Atlassian India LLP's (hereinafter referred as "Atlassian" or "Service Organization") system for providing Atlassian Focus to User Entities. The scope of the report does not include any other services or facilities of Atlassian other than those mentioned below. The scope of the report does not include projects/services that operate under the staff augmentation model.

The description is intended to provide users with information about the system supporting the services provided by Service Organization to meet the criteria for the Security, Availability and Confidentiality ("applicable trust services criteria") set forth in *TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*, as of 28 February 2025. Service Organization' Management is responsible for designing, implementing and documenting the controls to meet the applicable trust services criteria.

The description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user entity controls contemplated in the design of Service Organization controls are suitably designed, along with related controls at Service Organization. The period for SOC 2 Type I examination is as of 28 February 2025.

Overview Of Service Organization

Atlassian was established in 2002 by Scott Farquhar and Mike Cannon-Brookes and had its initial public offering (IPO) in 2015. Atlassian is committed to distributed teamwork, enabling employees to work remotely across various countries, with offices around the world including:

- The United States (Austin, Mountain View, New York City, San Francisco, Seattle)
- Australia (Sydney)
- Philippines (Manila)
- Japan (Yokohama)
- Netherlands (Amsterdam)
- Poland (Gdansk)
- Turkey (Ankara)
- India (Bengaluru)

Atlassian's ultimate goal 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.

This report focuses on the key operating systems that constitute the products and features hosted on Amazon Web Services (AWS) along with the supporting information technology (IT) infrastructure and business processes. It does not include on-premises versions such as Jira and Confluence Server and Data Center, service enhancements that are not explicitly defined, add-ons obtained from the marketplace, and open source downloadable added by customers to their instance.

SERVICES PROVIDED BY SERVICE ORGANIZATION TO USER ENTITIES

Below is the list of services provided by the Service Organization to User Entities.

Product Name	Details
Atlassian Focus	Atlassian Focus is an enterprise strategic portfolio management solution designed to help leaders and executives define, manage, and track their organization's strategic priorities. It serves as a central hub to map and align goals, work, teams, and funds with strategic priorities, providing visibility and enabling informed decision-making.

Sub Service Organization

Atlassian Focus utilizes AWS data centers and Infrastructure as a Service (IaaS). Atlassian administrators oversee virtual server and operating system configurations through distinct AWS accounts and configuration management processes.

SYSTEM OVERVIEW

Atlassian operates in a defined system to provide the technology services to User Entities. This system consists of multiple components such as policies and procedures, governance structure, support functions and application systems. The policies and procedures provide guidance to the users regarding the process to be followed for providing the services and assists in the consistent implementation of the same. The governance structure establishes a structure for operating the system and assists in demonstrating management commitment for the same. Information systems and supporting General Operating environment are implemented by Atlassian to support the processes followed to provide services to User Entities. Since Atlassian provides services to a variety of clients; most of them with unique requirements, this system operates at a higher level (which is independent of underlying client operations). Therefore, the description of system may not include every aspect of general operating controls that each client may consider important for its own environment.

Atlassian has established an internal controls framework that reflects:

- The overall control environment within the organization and its various processes
- The risk assessment procedure
- Control activities that help in meeting the overall control objectives
- Information and communication and
- Monitoring components of internal control

The components mentioned above are described in detail in the succeeding paragraphs. There is synergy and linkage among these components, forming an integrated system that responds dynamically to changing conditions. The internal control system is intertwined with the entity's operating activities and exists for fundamental business reasons. Internal control is most effective when controls are built into the entity's infrastructure and are a part of the essence of the enterprise. "Built in" controls support quality and empowerment initiatives, avoid unnecessary costs, and enable quick response to changing conditions.

COSO Framework

Atlassian operates a defined system to provide services to its User Entities. This system consists of multiple components such as policies and procedures, governance structure, support functions and application systems. The policies and procedures provide guidance to the users regarding the process to be followed for providing the services and assists in the consistent implementation of the same. The governance structure establishes a structure for operating the system and assists in demonstrating management commitment for the same.

The components mentioned above are described in additional detail in the succeeding paragraphs COSO (The Committee of Sponsoring Organizations of the Treadway Commission) is the internal control integrated framework that has been adopted by Atlassian to design and analyze its internal controls and for the presentation of this report. While internal control is a process, its effectiveness is a state or condition of the process at one or more moments in the timeline.

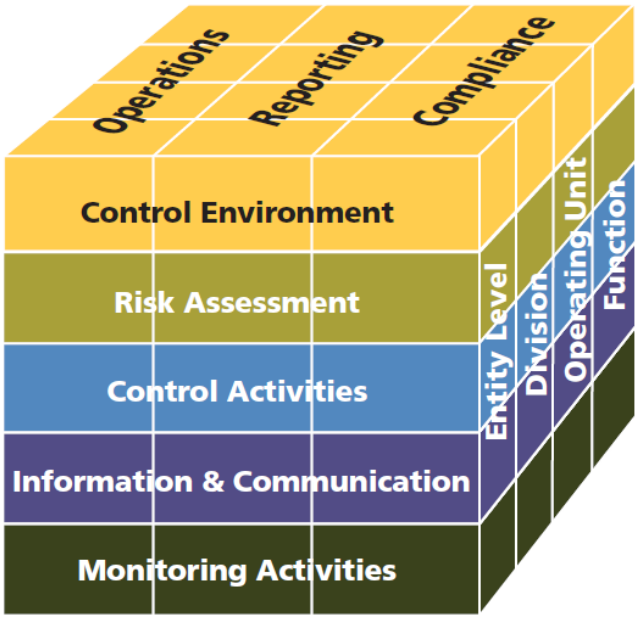

Figure 1: Components of Internal Control

Internal control consists of five interrelated components. These are derived from the way management runs a business and are integrated with the management process. The relevant aspects are described in detail in the succeeding paragraphs

The five components of internal control include:

- **Control Environment**: The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. The Board of Directors and senior management establish the tone at the top regarding the importance of internal control including expected standards of conduct. Management reinforces expectations at the various levels of the organization. The control environment comprises the integrity and ethical values of the organization; the parameters enabling the Board of Directors to carry out its governance oversight responsibilities; the Organizational Structure and assignment of authority and responsibility; the process for attracting, developing, and retaining competent individuals; and the rigor around performance measures, incentives and rewards to drive accountability for performance. The resulting control environment has a pervasive impact on the overall system of internal control.

- **Risk Assessment**: Every entity faces a variety of risks from external and internal sources. Risk is defined as the possibility that an event will occur and adversely affect the achievement of objectives. Risk assessment involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives. Risks to the achievement of these objectives from across the entity are considered relative to established risk tolerances. Thus, risk assessment forms the basis for determining how risks will be managed. A precondition to risk assessment is establishment of objectives, linked at different levels of the entity. Management specifies objectives within categories relating to operations, reporting and compliance with sufficient clarity to be able to identify and analyze risks to those objectives. Management also considers the suitability of the objectives for the entity. Risk assessment also requires management to consider the impact of possible changes in the external environment and within its own business model that may render internal control ineffective.

- **Control Activities**: Control activities are the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out. Control activities are performed at all levels of the entity, at various stages within business processes, and over the technology environment. They may be preventive or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations, and business performance reviews. Segregation of duties is typically built into the selection and development of control activities. Where segregation of duties is not practical, management selects and develops alternative control activities.

- **Information and Communication:** Information is necessary for the entity to carry out internal control responsibilities to support the achievement of its objectives. Management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of other components of

internal control. Communication is the continual, iterative process of providing, sharing, and obtaining necessary information. Internal communication is the means by which information is disseminated throughout the organization, flowing up, down, and across the entity. It enables personnel to receive a clear message from senior management that control responsibilities must be taken seriously. External communication is twofold: it enables inbound communication relevant external information, and it provides information to external parties in response to requirements and expectations.

- **Monitoring Activities:** Ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the five components of internal control, including controls to affect the principles within each component, is present and functioning. Ongoing evaluations, built into business processes at different levels of the entity, provide timely information. Separate evaluations, conducted periodically, will vary in scope and frequency depending on assessment of risks, effectiveness of ongoing evaluations, and other management considerations. Findings are evaluated against criteria established by regulators, recognized standard-setting bodies or management and the board of directors; deficiencies are communicated to management and the Board of Directors as appropriate. Internal control consists of five interrelated components. These are derived from the way management runs a business and are integrated with the management process.

There is synergy and linkage among these components, forming an integrated system that reacts dynamically to changing conditions. The internal control system is intertwined with the entity's operating activities and exists for fundamental business reasons.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Atlassian designs its processes and procedures related to technology services to meet its objectives. Those objectives are based on the service commitments agreed between Service Organization and User Entities, and applicable laws and regulations that govern the provision of said services.

COMPONENTS OF THE SYSTEM

Infrastructure

Atlassian products utilize AWS data centers and Infrastructure as a Service (IaaS). Atlassian administrators oversee virtual server and operating system configurations through distinct AWS accounts and configuration management processes.

Infrastructure - Products			
Products	**AWS Region(s)**		
	US	**EU**	**AP**
Atlassian Focus	✓		

Atlassian Focus also utilizes Atlassian's internally developed Micros Platform. Micros is Atlassian's Platform-as-a-Service (PaaS) solution designed to simplify the development and management of microservices for Atlassian developers. It provides a robust framework for provisioning services in the cloud, ensuring scalability, reliability, security.

Micros leverages AWS resources (e.g., EC2, CloudFormation) to deploy microservices within Docker containers; It supports multi-region deployments and advanced architectures; Automates tasks like DNS configuration, load balancing, database provisioning, and monitoring; provides out-of-the-box compliance, security, and observability tools; Developers provide a service descriptor and Docker images, and Micros handles the rest including resource provisioning and updates; Offers tools like Atlas CLI for seamless interaction with the platform.; Integrates with Atlassian's internal tools for logging, monitoring, and metrics aggregation.

Network

Atlassian has public ingress points in multiple AWS regions. These traffic manager clusters terminate public Transport Layer Security (TLS) and forward the request to proxies hosted in AWS regions. All AWS hosted network traffic is inside the Atlassian Cloud Network and all traffic in and between AWS regions uses AWS Transit Gateway or Amazon Virtual Private Cloud (Amazon VPC) peering. Encryption in transit is implemented to protect user authentication information and the

corresponding session transmitted over the Internet or other public networks to ensure that data reaches its intended destination.

Connections to features and products are protected using secure connectivity protocols. At all points, the network traffic is encrypted with TLS 1.2 or higher. Certificates have defined expiry dates that are notified and tracked internally so that they can be updated prior to their expiry.

Advanced Encryption Standard (AES)-256 is enabled to ensure encryption at rest within all data stores of Atlassian products and key services.

A Zero Trust infrastructure is implemented to place endpoints into a tiered network (High, Low, Open) based on their security posture and the type of device. Applications added to the Single Sign-On (SSO) platform are tiered according to the Zero Trust policy. Endpoints cannot access applications via the SSO platform unless they are placed on the same or higher tier as the application. High-tier applications have security requirements that include, but are not limited to, effective malware protection, local drive encryption, and up to date operating system versions.

Firewall rules have been implemented, and policy rules have been configured to restrict access to unnecessary ports, protocols, and services. Atlassian has implemented company-wide firewall rules that are managed centrally by the Micros Team. Individual products and features manage key Internet Protocol (IP) ports security policy roles to ensure that only authorized ports are in use. Any changes to firewall rules at the Global Edge, product, or feature level must go through a peer review and approval process.

Data

Atlassian products utilize logically separate databases for each product instance. The data is segregated by tenant at the application layer using a unique identifier to query customer data.

The databases implemented by Atlassian include independent synchronous replicas in multiple Availability Zones (AZs) within the same region to mitigate the risk of data loss due to hardware failure. The primary datastore used within the Atlassian environment consists of Amazon Relational Database Service (Amazon RDS) clusters located within the private network hosted in AWS. The cluster is shared, and its nodes are distributed across multiple AZs to provide fault tolerance and redundancy. Atlassian Focus also utilizes Atlassian's internally developed Transactional Data Platform for data storage.

Backups are retained at a minimum for 30 days to provide redundancy and enable point-in-time data recovery (PITR).

Software

Atlassian teams uses the following software to manage services being delivered to user entities. The scope of the report does not cover evaluation of design, implementation, and operating effectiveness of the tools mentioned below.

Function	Name
Hosting Systems	• Amazon EC2
Storage and Database	• Amazon RDS • Amazon DynamoDB
Network	• Amazon VPC • Amazon Load Balancers (ALB) • Amazon CloudFront • AWS Web Application Firewall (AWS WAF)

Function	Name
Application Cache	• Amazon ElastiCache
Encryption	• Amazon Key Management Services (KMS) • AWS Secret Manager
Messaging	• Amazon Simple Notification Service (Amazon SNS) • Amazon Simple Queue Service (Amazon SQS)
Build, Release, and Continuous Integration Systems	• Amazon Elastic Container Registry Service (Amazon ECR) • Bitbucket Cloud • Bitbucket Data Center • Bitbucket Pipelines • Deployment Bamboo • Docker • Metadata Platform • Tokenator
Access Management	• Active Directory (AD) • CyberArk Workforce Password Management • Duo two-factor authentication (2FA) • Okta SSO • 1Password
Monitoring and Alerting	• JSM Operations • Pollinator • SignalFX • Splunk
Customer Support and Communication	• Atlassian Developer Community • Statuspage
Vulnerability Scanning	• BugCrowd • CrowdStrike • Lacework • Snyk • Tenable

Function	Name
Human Resources (HR)	• Elevate • iCIMS • Workday
Learning, Training, and Development	• Absorb • LinkedIn Learning
Asset Management	• BitLocker • FileVaultl • Jamf Pro • Workspace One

The above-mentioned tools are owned and managed by Service Organization to provide the services to its clients and the scope of this report does not cover evaluation of design, implementation and operating effectiveness of the tools. The above-mentioned tools do not include client owned/ managed tools that Service Organization uses to provide the in-scope services.

People

The Company develops, manages, and secures Atlassian Focus via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
Co-Founder and Executive Management	Responsible for overseeing company-wide initiatives, establishing and accomplishing goals, and managing objectives
People (in partnership with the people leaders)	Responsible for determining career growth and performance strategy, talent acquisition, continuing education paths, total rewards, and workplace experiences
Finance	Responsible for financial, accounting, tax, Internal Audit, Investor Relations, Procurement, and Treasury
Legal	Responsible for matters related to corporate development, privacy, product counsel, general counsel operations, and public relations
Engineering	Responsible for the development, testing, deployment, and maintenance of new code for Atlassian products and features
Trust	Responsible for managing access controls, the security of the production environment, enterprise risk management, business continuity, and compliance for Atlassian products and features
Platform and Enterprise Cloud	Responsible for architecting, building, and maintaining Atlassian products and features

The following organizational chart reflects the Company's internal structure related to the groups discussed above:

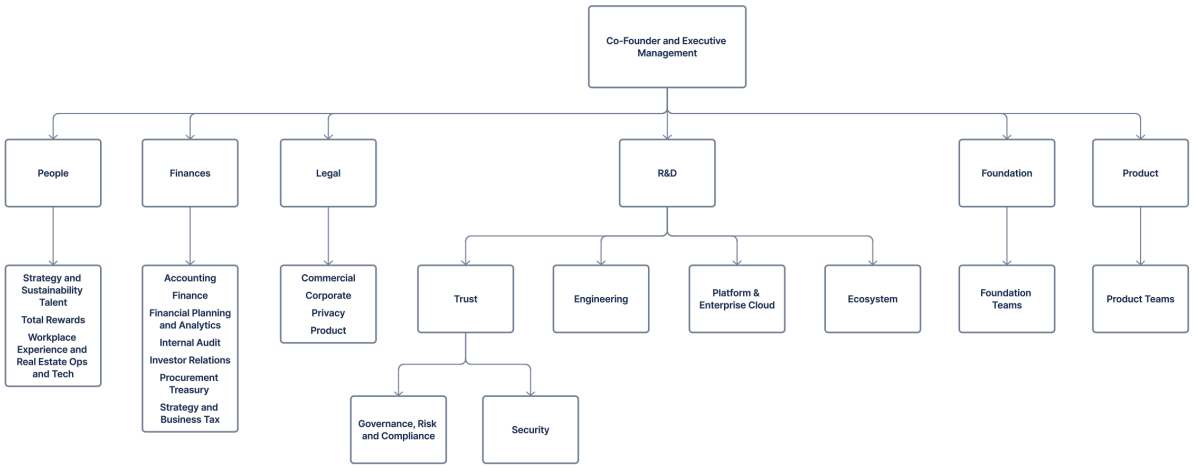

Figure 2: Atlassian Organizational Chart

Processes And Procedures

Atlassian maintains a Policy Management Program to help ensure that policies and procedures are:

- Properly communicated throughout the organization
- Properly owned, managed, and supported.
- Clearly outlining business objectives
- Showing commitment to meet regulatory obligations
- Focused on continual iteration and improvement.
- Providing for an exception process
- Supported by the Policy Framework and Structure

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

Policies, Standards, Guidelines, and Procedures		
Item	**Defines**	**Explanation**
Policy	General rules and requirements ("state")	Outlines specific requirements or rules that must be met.
Standard	Specific details ("what")	Collection of system-specific or procedural-specific requirements that must be met by all personnel.
Guideline	Common practice recommendations and suggestions	Collection of system specific or procedural specific "suggestions" for best practices. They are not requirements to be met but are strongly recommended. Effective policies make frequent references to standards and guidelines that exist within an organization.
Standard operating procedures	Steps to achieve Standard/Guideline requirements, in accordance with the rules ("actions")	Positioned underneath a standard or guideline, it is a set of instructions on how to accomplish a task. From a compliance perspective, a procedure is also referred to as a Control Activity: the goal of a process/procedure is to help

Policies, Standards, Guidelines, and Procedures		
		achieve a consistent outcome defined by the Standard or Guideline.
Policy	General rules and requirements (“state”)	Outlines specific requirements or rules that must be met.

Policy Requirements

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

Policy exceptions and violations are also reviewed by the APC and actions are recommended to the Policy Owners and Executive Management team. Policy owners can approve exceptions for a period no longer than one (1) year.

Policy Review Process

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

Data Classification and Confidentiality of Information

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

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

Data Classification		
Rating	**Description**	**Examples**
Restricted	Information that would be very damaging and would cause loss of trust with customers and present legal risk to Atlassian and/or customers if mishandled	• User Generated Content (UGC) • Restricted Personal Data • Sensitive company accounting data (e.g. non-public financial data, including consolidated revenue, expenses, cash flow, and earnings guidance prior to release) • Decryption keys, passwords, or other access control mechanisms protecting data at this level

Data Classification		
Protected	Information that could cause loss of trust with customers or present legal risk to Atlassian if mishandled	• Atlassian Account ID
Confidential	Information that would likely be damaging and could cause loss of trust with our customers if mishandled	• Confidential personal data elements • Information related to business plans or deals • Information under a Non-Disclosure Agreement (NDA) • Descriptions of unresolved security issues in Atlassian products • Third party closed-source code
Internal	Information internal to Atlassian that could be potentially damaging to Atlassian and/or customers if mishandled	• Most Confluence pages • Most information stored in Jira • Unreleased source code for Atlassian products • Unapproved drafts of public communications
Public	Data that is freely available to the public and presents no risk	• Approved public communications • Information on www.atlassian.com or other public web properties

CONTROL ENVIRONMENT

Integrity, Ethical Values and Competence

Integrity, ethical values, and competence are essential components of Atlassian's control environment. The People team is responsible for reviewing and monitoring compliance with these policies and agreements and ensuring that background screening procedures are carried out promptly.

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

Atlassian's Board of Directors and subcommittees meet annually to review committee charters, corporate governance, and strategic operational objectives. Meeting minutes are recorded with details on participants and dates. The Nominating and Governance Committee charter outlines the process for identifying candidates for the Board of Directors. Targets are conveyed to product groups for execution by Management, with progress evaluated quarterly. Audit committee information is accessible on Atlassian’s Investor website, including roles, responsibilities, key activities, meetings, qualifications for Financial Expert role, meeting calendar, and agenda developed annually with results published after each meeting.

Board and Governance Committee Charter

The Board of Directors and its subcommittees (Audit, Nominating and Governance, Compensation and Leadership Development) annually review the Audit, Board, and Nominating and Governance Committee Charters that outline their respective roles, responsibilities, meeting frequency, participants, member qualifications, discussion topics, and key activities. The Nominating and Governance Committee charter defines the process of identifying and reviewing candidates for the Board of Directors.

Management's Philosophy and Operating Style

At Atlassian, Executive and Senior Management are continuously engaged in a controlled environment. The Governance, Risk and Compliance team follows specific standards for security, availability, quality, reliability, and confidentiality. Customized tools assist in identifying risks and findings while workflows ensure proper tracking of activities. An Enterprise Risk Management process modeled after ISO 31000:2009 is used to create universal control activities that meet multiple standards. This approach promotes operational efficiency and a unified language across the organization.

Rules of Behaviour

Atlassian requires all employees and specified contractors to acknowledge the Code of Conduct, Insider Trading Policy, Foreign Corrupt Practices Act (FCPA) Agreement, and Anti-Corruption Policy upon hire to ensure that they are aware of their responsibilities and expected behavior. The comprehensive Code of Business Conduct and Ethics policy is reviewed on an annual basis. Atlassian ensures that all relevant personnel have appropriate access agreements in place.

A hotline for whistleblowers has been established and is available to both external individuals and Atlassian employees. It is included in the Code of Business Conduct, which all employees are required to acknowledge. Atlassian adheres to the Policy Violation Investigation Process when conducting investigations that may require disciplinary action, up to and including termination of employment, for individuals who fail to comply. Atlassian also requires its employees to complete workplace harassment training.

Personnel Management and Termination

Background checks are completed for new employees prior to their start date and a weekly review is conducted to confirm that the CIIA (Confidential Information and Inventions Assignment) has been signed as part of the onboarding process. Offers for external candidates are approved in Recruitment Central. The Talent Acquisition team approves offers for interns and graduates due to the bulk nature and timing of these hires.

Atlassian has a documented performance review process in place and reviews employee performance on an annual basis. Growth Plans are created to help employees understand expected attitudes, behavior, and skills that contribute to success in a role and connect them to resources aimed at improving those skills. Atlassian provides opportunities for professional development via training or tuition reimbursement and online learning management systems.

Atlassian has a documented Exit process in place which describes in detail the process for employee termination. Atlassian removes the access to the systems within 8 hours of users marked as inactive in Workday. Once access is removed, users will be unable to access the network, Wi-Fi, and VPN.

INFORMATION AND COMMUNICATION

Awareness and Training

Atlassian delivers annual security awareness and privacy training to all employees upon commencement of employment and annually thereafter. This program ensures staff are made aware of security and privacy risks, regulations and best practices. Automated notification reminders are sent to employees, contractors and escalated to their managers to make sure training is completed by the respective deadlines.

Program Management

Atlassian maintains comprehensive security policies, which are shared and reviewed annually to ensure that security is appropriately designed and integrated into the system. The policies are posted online, assigned a policy owner, and reviewed at least annually by the designated policy owner or their delegate.

An organizational chart is in place and updated to ensure clear identification of roles and responsibilities. The organizational chart is reviewed by appropriate Atlassian management and updated semi-annually.

Atlassian implements a process to ensure that strategic operational objectives are set, reviewed, and properly prioritized. The Executive Management team sets strategic operational objectives quarterly.

System Security Plan

Atlassian provides detailed documentation on system boundaries, product descriptions, and key features on both the Atlassian intranet and customer-facing website. Internal users and customers are informed of significant changes made to key products and features. Atlassian also communicates changes to security, availability and confidentiality commitments on its Atlassian Trust Center. For any material changes, an additional notice is also provided.

Incident Response

Atlassian maintains a company-wide incident management policy that is shared and reviewed on an annual basis. Incident management response procedures and plans are integrated into mission critical business processes and systems to minimize downtime, service degradation, and security risk for customers and internal users. System availability is published to provide assistance to users for the handling and reporting of incidents. Atlassian also provides a variety of methods and channels for customers to report incidents, system vulnerabilities, bugs, and issues related to defects, availability, security, and confidentiality.

Communication

Significant changes made to Atlassian Focus are communicated to internal users and customers. Atlassian communicates changes to confidentiality commitments through Atlassian's web site, when applicable.

RISK ASSESSMENT AND MITIGATION

Enterprise Risk Management

Atlassian's framework for enterprise risk management is developed, documented, and reviewed annually to manage risks related to Atlassian's strategy and business objectives. Atlassian has a comprehensive Risk Management policy that is shared, assigned a policy owner, and reviewed at least annually by the designated policy owner or their delegate. Atlassian has a well-defined risk assessment process in place in which risks are documented with a risk rating and assigned a risk owner. Atlassian ensures that risks outside of the acceptable level of risk are monitored and risk assessments are reviewed annually.

Fraud Risk Assessments

A fraud risk assessment is performed annually by the Enterprise Risk Management Team or a delegate. The assessment includes a cross functional survey of employees in areas susceptible to fraud combined with an evaluation of external risks. The report results are evaluated and communicated to executive level management and the Audit Committee.

Supplier Assessment and Review

Atlassian ensures that its vendors meet security, availability, and confidentiality commitments during the procurement process and on an ongoing basis, as applicable. Atlassian follows a defined process for vendor reviews, which includes an Initial Supplier Risk Assessment, Supplier Due Diligence and Risk Treatment, Contract Management, Supplier Monitoring. To achieve Atlassian's principal service commitments and system requirements, Atlassian reviews SOC reports at least annually for material third-party services and applications to ensure that controls are appropriate and operating effectively.

MONITORING

Internal Audit

The Internal Audit team is responsible for carrying out procedures to confirm adherence to and verification with the internal information security management system. The design of controls and mitigation strategies are reviewed on an annual basis. The outcomes of internal audits are documented, and corrective actions are monitored with regular reports to management.

Vulnerability Management

Atlassian performs code repository, container image, infrastructure, and cloud configuration vulnerability scanning on a continuous basis. Atlassian ensures that any legitimate vulnerabilities are remediated in accordance with the vulnerability management policy.

Penetration Testing

Atlassian conducts penetration testing on a continuous basis on all publicly accessible Atlassian products. Bug bounty programs are utilized to detect traditional web application vulnerabilities as well as other vulnerabilities that can have a direct impact. These vulnerabilities are tracked and mitigated until they are resolved.

Security Events Detection Monitoring

Atlassian performs reviews of logs to detect security events. Automated alerts are set up based on known and prior security events and incidents via Splunk. The Security Intelligence Team triages and investigates triggered alert. Incident Response Teams investigates the true positive events and take action as per the Incident Management process.

CONTROL ACTIVITIES

Access Control

Atlassian ensures that access to features, products, cloud service providers, internal systems, and tools is managed in compliance with relevant access control policies. Access is provisioned in line with the principle of least privilege only after approval is documented via a Jira ticket or in the internal Self Service Access Management (SSAM) tool and is reviewed at defined intervals. SSAM's are managed by the Container Owner and its delegates. Users are added to the SSAM containers directly by SSAM container Owner or the Container Delegates or requested by users and approved by the container Owner or the container delegates. SSAM containers also have the Just In Time (JIT) access where the access can be provided only for a specific amount of time. The Container owner is responsible for defining the roles and the requirement for each role.

Registration and de-registration of user access is restricted to authorized users via Active Directory (AD) group membership, which is automatically assigned based on the user's department and team. AD contains a subset of groups that are automatically created and maintained based on demographic and employment information in the HR Workday system. These groups are based on division, team, location, employment type, and management status. As well as initially provisioning membership, staff member's assigned groups are updated to reflect a team or department change or termination.

Identification and Authentication

Atlassian products and features are secured with passwords and multi-factor authentication (MFA). This ensures that only authorized individuals can access cloud services and remote access systems.

Atlassian employees are uniquely identified and authenticated using AD, which enforces password settings in accordance with the password standard. Atlassian's SSO portal (Okta) allows users to have a single point of authentication to access multiple applications.

In cases where MFA is not available, a distinct username and password must be provided. MFA is mandatory to access the virtual private network (VPN) from any IP address and when launching an application from Okta.

Customers are uniquely identified and authenticated as well using password mechanisms that are controlled by their Atlassian account. Unless an external identity provider is implemented by the customer, customers must meet the minimum password requirements that are controlled via their Atlassian account.

Network Security

Atlassian has firewall rules in place to restrict access to the production environment. The firewalls are configured to limit unnecessary ports, protocols, and services. Atlassian manages and monitors external interfaces and key internal interfaces to the products and features to prevent unauthorized use or access.

Malicious Code Protection

Atlassian implements and enforces malware protection on corporate endpoints. An enterprise anti-malware platform provides endpoint protection, centralized reporting, and notifications. Atlassian quarantines any malicious software upon detection of suspicious activities, and incident tickets are created for review and resolved in a timely manner.

Mobile Devices

Usage restrictions, configuration/connection requirements, and authorization are documented and established for mobile devices.

Encryption

Atlassian implements cryptographic mechanisms to prevent unauthorized disclosure and modification of data in transit and at rest.

Change Management

Atlassian ensures that configuration-controlled changes to products, features, and the infrastructure are reviewed, approved, and documented. Change management responsibilities are segregated among designated personnel. All changes are approved before deployment. Emergency changes also undergo a similar process.

Changes cannot be deployed unless it has passed the green build testing and have a compliance token. Changes are deployed to Artifactory and only docker images that exist in Artifactory will be replicated to container registry and then pushes the change to the production environment.

Changes are documented and monitored for non-compliance. An alert is automatically generated if a change to the peer review enforcement for pull requests occurs, assigned to the direct manager of the person who initiated the change and reviewed within defined timelines.

Prevention of Unauthorized Changes

Atlassian enforces restrictions on infrastructure access to prevent unauthorized modifications. Only Artifacts with a valid signature from build software can be released to the production environment. If unauthorized hardware, software, or firmware components are detected, they are isolated, and access is disabled until the relevant support personnel are notified. IT Asset management software is utilized to enforce hard drive encryption, user authentication requirements, and security patching on MacOS and Windows endpoints.

Availability

Contingency Planning and Backups

Atlassian has a comprehensive disaster recovery policy that has been assigned a policy owner and is reviewed at least annually by the designated policy owner or their delegate. It outlines the purpose, objectives, scope, critical dependencies, recovery time objective/recovery point objective (RTO/RPO), and roles and responsibilities. These details are also available online on the Atlassian Trust Center.

Atlassian conducts quarterly disaster recovery tests and performs exercises to help disaster response teams walk through various scenarios. Post testing, outputs are captured and analyzed to determine next steps for continued improvement.

Atlassian performs backups and periodic restoration testing of system data for its products and features to ensure that data security, integrity, and reliability are maintained. Capacity management is performed on an ongoing basis by all products. Changes to the availability and processing capacity of the customer-facing service products and key features are internally monitored and adjusted accordingly.

In the event of a catastrophic failure, Atlassian has break glass procedures in place to bypass MFA required for the VPN and the Atlassian SSO portal (Okta).

Confidentiality

Information Handling and Retention

Atlassian ensures that customer data is deleted within a reasonable time frame upon request or termination of contract. Upon termination of contract, the customer's account is deactivated after the end of the customer's current subscription period. Atlassian retains data for deactivated products for up to 60 days at the end of the customer's current subscription period. Upon deletion, an archive of the data is kept for at a minimum for an additional 30 days.

Access to Customer Data

Customer data is logically isolated through the use of unique identifiers. Access to customer data is granted implicitly through customer support tickets or active incidents. This access is for troubleshooting purposes and is granted via tokens only for a limited period of time or until the incident is closed. Customer support tickets can only be submitted by individuals delegated as administrators within Atlassian Admin.

COMPLEMENTARY USER ENTITY CONTROLS

In the design of its controls, Atlassian has envisaged certain controls to be exercised by the user entity (complementary user entity controls). The responsibility for design, implementation and operating effectiveness of these controls' rests with the user entity. This information has been provided to user entities and to their auditors to be taken into consideration when making assessments of control risk for the user entity. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls. For user entities to rely on the controls reported herein, each user entity must evaluate its own internal control to determine whether the identified CUECs have been implemented and are operating effectively.

The CUECs presented should not be regarded as a comprehensive list of all controls that should be employed by user entities. Management of user entities is responsible for the following:

Criteria	Complementary User Entity Controls
CC2.1	User Entities are responsible for identifying approved points of contacts to coordinate with Atlassian. User Entities are responsible for the security and confidentiality of the data submitted on Atlassian support tickets.
CC2.3	User Entities are responsible for assessing and evaluating any potential impact add-ons may have on their instance.
CC6.1	User Entities are responsible for configuring their own instance, including the appropriate set-up of their logical security and privacy settings (such as IP allowed listing, 2FA, SSO setup, password settings, and restricting public access). User Entities are responsible for changing their passwords to reflect a minimum length of at least eight (8) characters where they have migrated from another identity service. User Entities are responsible for the safeguarding of their own account access credentials, including passwords or Application Programming Interface (API) keys and tokens.
CC6.6 CC6.8 C1.1 C1.2	User Entities are responsible for security, including virus scans and confidentiality of the data (e.g., media attachments), prior to import or attachment and its ongoing monitoring after data has been uploaded.
CC6.2 CC6.3	User Entities are responsible for managing access rights, including privileged access. User Entities are responsible for requesting, approving, and monitoring Atlassian's customer support access to their account.
CC6.2	User Entities are responsible for requesting removal of their account.

Criteria	Complementary User Entity Controls
CC6.3 C1.2	
CC6.6 CC6.7 CC6.8	User Entities are responsible for ensuring that their machines, devices, and network are secured.
CC7.3	User Entities are responsible for alerting Atlassian of incidents (related to security, availability, and confidentiality) when they become aware of them.

COMPLEMENTARY SUB-SERVICE ORGANIZATION CONTROLS

The Company uses AWS as a subservice organization for data center colocation services. The Company's controls related to Atlassian Focus cover only a portion of the overall internal control for each user entity of the products and features. The description does not extend to the colocation services for IT infrastructure provided by the subservice organization. The description of the system only covers the Trust Services Criteria and related controls of the Company and exclude the related controls of AWS.

Although the subservice organization has been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organization. CSOCs are expected to be in place at AWS related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. AWS' physical security controls should mitigate the risk of unauthorized access to the hosting facilities. AWS' environmental protection controls should mitigate the risk of fires, power loss, climate, and temperature variabilities.

Company management receives and reviews the AWS SOC 2 report annually. In addition, through its operational activities, Company management monitors the services performed by AWS to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organization to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to AWS management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to Atlassian Focus to be achieved solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls, considering the related CSOCs expected to be implemented at AWS as described below.

Criteria	Complementary Subservice Organization Controls
	AWS is responsible for IT access above least privileged, including administrator access.
CC6.1	AWS is responsible for approval by appropriate personnel prior to access provisioning.
CC6.2	AWS is responsible for privileged IT access reviews on a regular basis.
CC6.3	AWS is responsible for timely revocation of user access upon termination.
	AWS is responsible for encrypting data in transit.

Criteria	Complementary Subservice Organization Controls
CC6.4	AWS is responsible for restricting physical access to the computer rooms that house the entity's IT resources, servers, and related hardware to authorized individuals through a badge access system or equivalent that is monitored by video surveillance. AWS is responsible for approving requests for physical access privileges from an authorized individual. AWS is responsible for requiring visitors to be signed in by an authorized workforce member before gaining entry and for always escorting approved visitors.
CC6.5 CC6.7	AWS is responsible for securely decommissioning and physically destroying production assets in their control.
CC7.1 CC7.2 CC7.3	AWS is responsible for implementing and monitoring electronic intrusion detection systems that can detect breaches into data center server locations. AWS is responsible for documenting procedures for the identification and escalation of potential security breaches.
CC7.2 A1.2	AWS is responsible for installing environmental protection that includes the following: cooling systems, battery and generator backups, smoke detection, and dry pipe sprinklers. AWS is responsible for monitoring the environmental protection equipment for incidents or events that impact assets.
CC8.1	AWS is responsible for ensuring that changes are authorized, tested, and approved prior to implementation.

MAPPING OF SOC2 TRUST SERVICES CRITERIA WITH CONTROL ACTIVITIES

Trust Service Criteria		Control Activities
CC 1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Atlassian has defined a Comprehensive Code of Business Conduct and Ethics Policy which describes the employee and contractor responsibilities and expected behaviour regarding data and information system usage. The Policy is shared to all employee online and reviewed on an annual basis.
		New employees and contractors acknowledge the Code of Business Conduct, Insider Trading Policy, and FCPA (Foreign Corrupt Practices Act) and Anti-Corruption Policy upon hire.
		Atlassian employees and contractors are required to sign Confidential Information and Invention Assignments (CIIA) as part of their onboarding process.
		Background checks are performed prior to a new hire's start date in compliance with local laws and regulations.
		A weekly review is performed to determine that the CIIA (Confidential Information and Inventions Assignment) and background checks are completed for new employees prior to their start date.
		Atlassian employees are rewarded and recognised for their contribution and accomplishments as a part of their annual performance review process.
		Atlassian has documented the process of identifying and reviewing Board of Director candidates in the Nominating and Governance Committee charter.
		The Board of Directors reviews the committee charters and corporate governance which define their roles, responsibilities, meeting frequency, participants, member qualifications, and discussion topics at least annually.
		Vendors and associated security, availability and confidentiality commitments are reviewed by appropriate Atlassian management during the procurement process and on an ongoing basis, as applicable. **Exception Noted:** It was noted that for a sample vendor, while a contract termination request process exists and is documented, a comprehensive vendor off-boarding process is not currently established and tracked via tickets. **Management Response:** Management is formalizing a comprehensive process to track the off boarding of vendors.
CC 1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Atlassian has documented the process of identifying and reviewing Board of Director candidates in the Nominating and Governance Committee charter.
		The Board of Directors reviews the committee charters and corporate governance which define their roles, responsibilities, meeting frequency, participants, member qualifications, and discussion topics at least annually.
		Atlassian has defined audit committee meeting calendar and agenda.
		Atlassian has defined an audit committee charter outlining their roles, responsibilities and key activities.

Trust Service Criteria		Control Activities
CC 1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The organizational charts are reviewed by appropriate Atlassian management and updated semi-annually.
		Organizational charts are updated based on employee transactions. Organizational charts are available to all Atlassian employees via Workday.
		The signature authority matrix is maintained by Procurement and Legal which establishes the signature authority for expenditures, contracts, and capital acquisitions.
		Vendors and associated security, availability and confidentiality commitments are reviewed by appropriate Atlassian management during the procurement process and on an ongoing basis, as applicable. **Exception Noted:** It was noted that for a sample vendor, while a contract termination request process exists and is documented, a comprehensive vendor off-boarding process is not currently established and tracked via tickets. **Management Response:** Management is formalizing a comprehensive process to track the off boarding of vendors.
		Atlassian has documented the process of identifying and reviewing Board of Director candidates in the Nominating and Governance Committee charter.
		The Board of Directors reviews the committee charters and corporate governance which define their roles, responsibilities, meeting frequency, participants, member qualifications, and discussion topics at least annually.
		Hiring Manager or Talent Acquisition Operations (TA Ops) team reviews and approves the job description posted for job ads.
CC 1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	On an annual basis, Atlassian employees undergo Security Awareness Trainings as part of the Atlassian Security Awareness Program. If an employee or contractor has not completed their privacy training within the expected timeframe, notification reminders will be sent to the employee/contractor and their manager to complete the training program.
		New joiners are required to complete Security awareness training within 30 days of joining as part of the Atlassian Security Awareness Program. If an employee or contractor has not completed their privacy training within the expected timeframe, notification reminders will be sent to the employee/contractor and their manager to complete the training program.
		Atlassian's Trust & Security Team hosts regular knowledge sharing and awareness sessions. These are facilitated and presented by Managers and Individual Contributors.
		Atlassian provides trainings to their employees to support their continued development and growth.
		Atlassian employees and contractors are required to sign Confidential Information and Invention Assignments (CIIA) as part of their onboarding process.

Trust Service Criteria		Control Activities
		Background checks are performed prior to a new hire's start date in compliance with local laws and regulations.
		Every external offer that goes out is formally approved in Recruitment Central prior to receiving an offer.
		Atlassian has documented the process of identifying and reviewing Board of Director candidates in the Nominating and Governance Committee charter.
		A weekly review is performed to determine that the CIIA (Confidential Information and Inventions Assignment) and background checks are completed for new employees prior to their start date.
		New employees and contractors acknowledge the Code of Business Conduct, Insider Trading Policy, and FCPA (Foreign Corrupt Practices Act) and Anti-Corruption Policy upon hire.
		The Board of Directors reviews the committee charters and corporate governance which define their roles, responsibilities, meeting frequency, participants, member qualifications, and discussion topics at least annually.
		Atlassian employees are rewarded and recognised for their contribution and accomplishments as a part of their annual performance review process.
CC 1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Atlassian employees are rewarded and recognised for their contribution and accomplishments as a part of their annual performance review process.
		Atlassian has defined a Comprehensive Code of Business Conduct and Ethics Policy which describes the employee and Contractor responsibilities and expected behaviour regarding data and information system usage. The policy is shared to all employee online and reviewed on an annual basis.
		Atlassian provides trainings to their employees to support their continued development and growth.
		New employees and contractors acknowledge the Code of Business Conduct, Insider Trading Policy, and FCPA (Foreign Corrupt Practices Act) and Anti-Corruption Policy upon hire.
		The Company has documented disciplinary process in place for employees and contractors who violate the Atlassian Code of Business Conduct and Ethics.

Trust Service Criteria		Control Activities
CC 2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Atlassian has defined a Policy Management Program (PMP) to ensure policies are reviewed at least annually by the designated policy owner or their delegate and are available online.
		Atlassian Focus maintains a data flow map for their systems and services that process personal data.
		Atlassian employees and contractors are required to sign Confidential Information and Invention Assignments (CIIA) as part of their onboarding process.

Trust Service Criteria		Control Activities
		Atlassian Endpoint assets are recorded, assigned, and tracked using the Jira asset tracking project (TAG).
		TDP maintains a data flow map for their systems and services that process personal data.
		Atlassian has implemented secure disposal and re-use of equipment policy. Agreements are in place to manage procedures to sanitise, and wipe used Atlassian issued devices prior to repurposing.
CC 2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	On an annual basis, Atlassian employees undergo Security Awareness Trainings as part of the Atlassian Security Awareness Program. If an employee or contractor has not completed their privacy training within the expected timeframe, notification reminders will be sent to the employee/contractor and their manager to complete the training program.
		The Atlassian Executive team reviews, sets, and/or revises strategic operational objectives quarterly as focus areas during the State of Atlassian (SoA) and Rolling 4 (R4) sessions. The targets are cascaded down into each of the product groups for execution by the Management Team.
		Atlassian has established a Whistleblower hotline that is accessible to both external individuals and employees within the Company.
		The organizational charts are reviewed by appropriate Atlassian management and updated on a semi-annually basis.
		Atlassian's Trust & Security Team hosts regular knowledge sharing and awareness sessions. These are facilitated and presented by Managers and Individual Contributors.
		Atlassian communicates changes to confidentiality commitments through Atlassian's web site.
		Atlassian communicates its commitment to security as a priority for its customers via Atlassian Trust Security page.
		Incidents are recorded in the Incident Management Systems. For Major, Critical and Crisis Incidents (i.e., severity 2 and above), a Post Incident Review (PIR) is completed by SRE (Site Reliability Engineering) team.
		Atlassian has defined audit committee meeting calendar and agenda.
		Atlassian has defined an audit committee charter outlining their roles, responsibilities and key activities.
		The Board of Directors reviews the committee charters and corporate governance which define their roles, responsibilities, meeting frequency, participants, member qualifications, and discussion topics at least annually.
		A description of the system delineating the boundaries and describing relevant components of Atlassian focus is documented on the Atlassian intranet and the system features and functionality of Atlassian Focus is documented on the customer-facing Atlassian website.

Trust Service Criteria		Control Activities
		Significant changes made to Atlassian Focus are communicated to internal users and customers.
CC 2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	Internal or External users can report bugs, defects, or security, confidentiality and availability issues via Atlassian approved communication channels.
		Customer terms of service (ToS) are standardized and approved by legal. The ToS communicate Atlassian's security, availability and confidentiality commitments and the customer responsibilities and obligations. Any changes to these commitments or responsibilities in the ToS are communicated to customers pursuant to the notification procedures specified in the ToS.
		Vendors and associated security, availability and confidentiality commitments are reviewed by appropriate Atlassian management during the procurement process and on an ongoing basis, as applicable. **Exception Noted:** It was noted that for a sample vendor, while a contract termination request process exists and is documented, a comprehensive vendor off-boarding process is not currently established and tracked via tickets. **Management Response:** Management is formalizing a comprehensive process to track the off boarding of vendors.
		Atlassian has established a Whistleblower hotline that is accessible to both external individuals and employees within the Company.
		Atlassian communicates its commitment to security as a priority for its customers via Atlassian Trust Security page.
		Atlassian communicates changes to confidentiality commitments through Atlassian's web site.
		The Atlassian Executive team reviews, sets, and/or revises strategic operational objectives quarterly as focus areas during the State of Atlassian (SoA) and Rolling 4 (R4) sessions. The targets are cascaded down into each of the product groups for execution by the Management Team.
		New employees and contractors acknowledge the Code of Business Conduct, Insider Trading Policy, and FCPA (Foreign Corrupt Practices Act) and Anti-Corruption Policy upon hire.
		Atlassian has defined audit committee meeting calendar and agenda.
		Atlassian has defined an audit committee charter outlining their roles, responsibilities and key activities.
		A description of the system delineating the boundaries and describing relevant components of Atlassian focus is documented on the Atlassian intranet and the system features and functionality of Atlassian Focus is documented on the customer-facing Atlassian website.
		Significant changes made to Atlassian Focus are communicated to internal users and customers.

Trust Service Criteria		Control Activities
		Changes to system availability is published externally to allow customers to check the status/uptime of Atlassian Focus in real-time.
		The Board of Directors reviews the committee charters and corporate governance which define their roles, responsibilities, meeting frequency, participants, member qualifications, and discussion topics at least annually.

Trust Service Criteria		Control Activities
CC 3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The Atlassian Executive team reviews, sets, and/or revises strategic operational objectives quarterly as focus areas during the State of Atlassian (SoA) and Rolling 4 (R4) sessions. The targets are cascaded down into each of the product groups for execution by the Management Team.
		The Board of Directors reviews the committee charters and corporate governance which define their roles, responsibilities, meeting frequency, participants, member qualifications, and discussion topics at least annually.
		Atlassian has defined a Risk Assessment process document. The document is reviewed and approved on an annual basis.
		Atlassian develops and documents action plans associated with Enterprise Risks. Risk reviews are performed as per Atlassian Enterprise Risk Management capability document. **Exception Noted:** It was noted that for a selected risk, risk treatment plan and risk review were not performed in line with the Atlassian Enterprise Risk Management Policy. **Management Response:** Management identified the selected risk did not require a risk treatment plan as it should have been moved to an archived state. Management is in the process of migrating to a new risk tracking system as part of GRC tooling uplift that will enhance our risk management processes.
		Atlassian Internal Audit team prepares the results of the financial statement risk assessment and shares with the Head of Finance and Accounting for validation on an annual basis.
		Internal Audit performs audits on an annual basis. The results of internal audits are captured, and remediation is tracked with regular reports to management.
		The signature authority matrix is maintained by Procurement and Legal which establishes the signature authority for expenditures, contracts, and capital acquisitions.
		Review of financial statements and footnote disclosures is performed by Head of Technical Accounting.
		Atlassian Enterprise Risk Management Team performs fraud risk assessment on an annual basis. Results are reviewed and communicated to senior stakeholders.

Trust Service Criteria		Control Activities
CC 3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyses risks as a basis for determining how the risks should be managed.	Atlassian has defined a Risk Assessment process document. The document is reviewed and approved on an annual basis.
		Atlassian develops and documents action plans associated with Enterprise Risks. Risk reviews are performed as per Atlassian Enterprise Risk Management capability document. **Exception Noted:** It was noted that for a selected risk, risk treatment plan and risk review were not performed in line with the Atlassian Enterprise Risk Management Policy. **Management Response:** Management identified the selected risk did not require a risk treatment plan as it should have been moved to an archived state. Management is in the process of migrating to a new risk tracking system as part of GRC tooling uplift that will enhance our risk management processes.
		Internal Audit performs audits on an annual basis. The results of internal audits are captured, and remediation is tracked with regular reports to management.
		Atlassian Enterprise Risk Management Team performs fraud risk assessment on an annual basis. Results are reviewed and communicated to senior stakeholders.
		Atlassian Internal Audit team prepares the results of the financial statement risk assessment and shares with the Head of Finance and Accounting for validation on an annual basis.
		Vendors and associated security, availability and confidentiality commitments are reviewed by appropriate Atlassian management during the procurement process and on an ongoing basis, as applicable. **Exception Noted:** It was noted that for a sample vendor, while a contract termination request process exists and is documented, a comprehensive vendor off-boarding process is not currently established and tracked via tickets. **Management Response:** Management is formalizing a comprehensive process to track the off boarding of vendors.
		Penetration testing is performed by Atlassian using Bug Bounty on a continuous basis. The Vulnerabilities identified are tracked and resolved in accordance with the Vulnerability Management process document.
		Atlassian performs the container image scanning to identify vulnerable software in container images. Identified vulnerabilities are tracked and resolved in accordance with the Atlassian Vulnerability Management process document.
		Atlassian performs the software composition analysis to automatically scan code repositories for known vulnerabilities in third party dependencies. Identified vulnerabilities are tracked and resolved in accordance with the Atlassian Vulnerability Management process document.
		Atlassian performs the cloud configuration monitoring to scan AWS account configurations against a defined ruleset. Identified vulnerabilities are tracked and

Trust Service Criteria		Control Activities
		resolved in accordance with the Atlassian Vulnerability Management process document.
		Atlassian performs the host-based vulnerabilities to perform host-based scans of its infrastructure. Identified vulnerabilities are tracked and resolved in accordance with the Atlassian Vulnerability Management process document.
		Atlassian reviews SOC reports at least annually for material third party services and applications to ensure controls are appropriate and operating effectively as defined in Standard - Vendor Service Organisation Control (SOC) Report Review process document.
CC 3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Atlassian has defined a Risk Assessment process document. The document is reviewed and approved on an annual basis.
		Atlassian develops and documents action plans associated with Enterprise Risks. Risk reviews are performed as per Atlassian Enterprise Risk Management capability document. **Exception Noted:** It was noted that for a selected risk, risk treatment plan and risk review were not performed in line with the Atlassian Enterprise Risk Management Policy. **Management Response:** Management identified the selected risk did not require a risk treatment plan as it should have been moved to an archived state. Management is in the process of migrating to a new risk tracking system as part of GRC tooling uplift that will enhance our risk management processes.
		Penetration testing is performed by Atlassian using Bug Bounty on a continuous basis. The Vulnerabilities identified are tracked and resolved in accordance with the Vulnerability Management process document.
		Atlassian performs the container image scanning to identify vulnerable software in container images. Identified vulnerabilities are tracked and resolved in accordance with the Atlassian Vulnerability Management process document.
		Atlassian performs the software composition analysis to automatically scan code repositories for known vulnerabilities in third party dependencies. Identified vulnerabilities are tracked and resolved in accordance with the Atlassian Vulnerability Management process document.
		Atlassian performs the cloud configuration monitoring to scan AWS account configurations against a defined ruleset. Identified vulnerabilities are tracked and resolved in accordance with the Atlassian Vulnerability Management process document.
		Atlassian performs the host-based vulnerabilities to perform host-based scans of its infrastructure. Identified vulnerabilities are tracked and resolved in accordance with the Atlassian Vulnerability Management process document.
		Atlassian Internal Audit team prepares the results of the financial statement risk assessment and shares with the Head of Finance and Accounting for validation on an annual basis.

Trust Service Criteria		Control Activities
		Atlassian Enterprise Risk Management Team performs fraud risk assessment on an annual basis. Results are reviewed and communicated to senior stakeholders.
CC 3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Atlassian has defined a Risk Assessment process document. The document is reviewed and approved on an annual basis.
		Atlassian develops and documents action plans associated with Enterprise Risks. Risk reviews are performed as per Atlassian Enterprise Risk Management capability document. **Exception Noted:** It was noted that for a selected risk, risk treatment plan and risk review were not performed in line with the Atlassian Enterprise Risk Management Policy. **Management Response:** Management identified the selected risk did not require a risk treatment plan as it should have been moved to an archived state. Management is in the process of migrating to a new risk tracking system as part of GRC tooling uplift that will enhance our risk management processes.
		Atlassian reviews SOC reports at least annually for material third party services and applications to ensure controls are appropriate and operating effectively as defined in Standard - Vendor Service Organisation Control (SOC) Report Review process document.
		Vendors and associated security, availability and confidentiality commitments are reviewed by appropriate Atlassian management during the procurement process and on an ongoing basis, as applicable. **Exception Noted:** It was noted that for a sample vendor, while a contract termination request process exists and is documented, a comprehensive vendor off-boarding process is not currently established and tracked via tickets. **Management Response:** Management is formalizing a comprehensive process to track the off boarding of vendors.
		Atlassian performs periodic review of on-going changes to privacy laws and regulations.
		The Atlassian Executive team reviews, sets, and/or revises strategic operational objectives quarterly as focus areas during the State of Atlassian (SoA) and Rolling 4 (R4) sessions. The targets are cascaded down into each of the product groups for execution by the Management Team.
		Penetration testing is performed by Atlassian using Bug Bounty on a continuous basis. The Vulnerabilities identified are tracked and resolved in accordance with the Vulnerability Management process document.
		Atlassian performs the container image scanning to identify vulnerable software in container images. Identified vulnerabilities are tracked and resolved in accordance with the Atlassian Vulnerability Management process document.
		Atlassian performs the software composition analysis to automatically scan code repositories for known vulnerabilities in third party dependencies. Identified

Trust Service Criteria		Control Activities
		vulnerabilities are tracked and resolved in accordance with the Atlassian Vulnerability Management process document.
		Atlassian performs the cloud configuration monitoring to scan AWS account configurations against a defined ruleset. Identified vulnerabilities are tracked and resolved in accordance with the Atlassian Vulnerability Management process document.
		Atlassian performs the host-based vulnerabilities to perform host-based scans of its infrastructure. Identified vulnerabilities are tracked and resolved in accordance with the Atlassian Vulnerability Management process document.
		Atlassian Enterprise Risk Management Team performs fraud risk assessment on an annual basis. Results are reviewed and communicated to senior stakeholders.

Trust Service Criteria		Control Activities
CC 4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Internal Audit performs audits on an annual basis. The results of internal audits are captured, and remediation is tracked with regular reports to management.
		Atlassian reviews SOC reports at least annually for material third party services and applications to ensure controls are appropriate and operating effectively as defined in Standard - Vendor Service Organisation Control (SOC) Report Review process document.
		Based on the data shared with the third party, Atlassian third party contract outlines the required security and privacy controls.
		Penetration testing is performed by Atlassian using Bug Bounty on a continuous basis. The Vulnerabilities identified are tracked and resolved in accordance with the Vulnerability Management process document.
		Atlassian performs the container image scanning to identify vulnerable software in container images. Identified vulnerabilities are tracked and resolved in accordance with the Atlassian Vulnerability Management process document.
		Atlassian performs the software composition analysis to automatically scan code repositories for known vulnerabilities in third party dependencies. Identified vulnerabilities are tracked and resolved in accordance with the Atlassian Vulnerability Management process document.
		Atlassian performs the cloud configuration monitoring to scan AWS account configurations against a defined ruleset. Identified vulnerabilities are tracked and resolved in accordance with the Atlassian Vulnerability Management process document.
		Atlassian performs the host-based vulnerabilities to perform host-based scans of its infrastructure. Identified vulnerabilities are tracked and resolved in accordance with the Atlassian Vulnerability Management process document.
CC 4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a	Internal Audit performs audits on an annual basis. The results of internal audits are captured, and remediation is tracked with regular reports to management.
		Atlassian has defined audit committee meeting calendar and agenda.

Trust Service Criteria		Control Activities
	timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Atlassian has defined an audit committee charter outlining their roles, responsibilities and key activities.
		Review of financial statements and footnote disclosures is performed by Head of Technical Accounting.
		Atlassian reviews SOC reports at least annually for material third party services and applications to ensure controls are appropriate and operating effectively as defined in Standard - Vendor Service Organisation Control (SOC) Report Review process document.

Trust Service Criteria		Control Activities
CC 5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Atlassian has defined a Risk Assessment process document. The document is reviewed and approved on an annual basis.
		Atlassian develops and documents action plans associated with Enterprise Risks. Risk reviews are performed as per Atlassian Enterprise Risk Management capability document. **Exception Noted:** It was noted that for a selected risk, risk treatment plan and risk review were not performed in line with the Atlassian Enterprise Risk Management Policy. **Management Response:** Management identified the selected risk did not require a risk treatment plan as it should have been moved to an archived state. Management is in the process of migrating to a new risk tracking system as part of GRC tooling uplift that will enhance our risk management processes.
		Internal Audit performs audits on an annual basis. The results of internal audits are captured, and remediation is tracked with regular reports to management.
		Atlassian Enterprise Risk Management Team performs fraud risk assessment on an annual basis. Results are reviewed and communicated to senior stakeholders.
		The signature authority matrix is maintained by Procurement and Legal which establishes the signature authority for expenditures, contracts, and capital acquisitions.
		Atlassian Internal Audit team prepares the results of the financial statement risk assessment and shares with the Head of Finance and Accounting for validation on an annual basis.
CC 5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Atlassian has defined a Risk Assessment process document. The document is reviewed and approved on an annual basis.
		Atlassian develops and documents action plans associated with Enterprise Risks. Risk reviews are performed as per Atlassian Enterprise Risk Management capability document. **Exception Noted:**

Trust Service Criteria		Control Activities
		It was noted that for a selected risk, risk treatment plan and risk review were not performed in line with the Atlassian Enterprise Risk Management Policy. **Management Response:** Management identified the selected risk did not require a risk treatment plan as it should have been moved to an archived state. Management is in the process of migrating to a new risk tracking system as part of GRC tooling uplift that will enhance our risk management processes.
		A formal disaster recovery plan is in place for Atlassian Focus systems which is reviewed and tested on a quarterly basis in accordance with the Atlassian BC/DR (Business Continuity/Disaster Recovery) program. Atlassian Focus teams completes a business impact analysis on a periodic basis to identify recovery objectives and classify services.
		Privileged access of Atlassian users to EC2 production environment is restricted to authorized and appropriate users only.
		The Root user password for all AWS management accounts meets password settings as defined in Standard - Passwords.
		Active Directory enforces password settings in line with the Atlassian Password Standard.
		Internal Audit performs audits on an annual basis. The results of internal audits are captured, and remediation is tracked with regular reports to management.
		A formal disaster recovery plan is in place for TDP systems which is reviewed and tested on a quarterly basis in accordance with the Atlassian BC/DR (Business Continuity/Disaster Recovery) program. TDP teams completes a business impact analysis on a periodic basis to identify recovery objectives and classify services.
CC 5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Atlassian has defined a Comprehensive Code of Business Conduct and Ethics Policy which describes the employee and Contractor responsibilities and expected behaviour regarding data and information system usage. The policy is shared to all employee online and reviewed on an annual basis.
		Atlassian has defined a formal procedure that outline the process to perform the following system access controls functions: - Access Provisioning, - Access Modification, - Access Revocation, - Restriction of access based on Segregation of Duties and least privilege. The document is shared to all employee online and reviewed on an annual basis.
		Atlassian has defined a procurement policy which describes the vendor management process in detail. The policy is shared to all employee online and reviewed on an annual basis.
		Atlassian has defined a Privacy Policy which describes on how Atlassian implements appropriate security measures to help protect data privacy in detail. The policy is shared to all employee online and reviewed on an annual basis.

Trust Service Criteria		Control Activities
		Atlassian has defined an Incident Management Policy which describes the Incident Management process on how Atlassian responds to customer downtime or degraded service in detail. The policy is shared to all employee online and reviewed on an annual basis.
		Atlassian has defined a Security Incident Management Policy. The policy is shared to all employee online and reviewed on an annual basis.
		Atlassian has defined a Software Development Lifecycle policy which describes the development, acquisition, implementation, changes, and maintenance of information systems and related technology requirements. The policy is shared to all employee online and reviewed on an annual basis.
		Atlassian has defined a Threat and Vulnerability Management policy which describes in detail the vulnerability management and systems monitoring process in detail. The policy is shared to all employee online and reviewed on an annual basis.
		Atlassian has defined a Data Classification policy which describes the system of data classification for operational use at Atlassian in detail. The policy is shared to all employee online and reviewed on an annual basis.
		Atlassian has defined a Background Check policy which describes the guidelines for background checks to be performed at Atlassian in detail. The policy is shared to all employee online and reviewed on an annual basis.
		Atlassian has defined a Change Management Policy which describes the process managing systems and services related changes in detail. The policy is shared to all employee online and reviewed on an annual basis. **Exception Noted:** It was noted that the policy document "standard – Change Management" was not reviewed by the designated policy owner. **Management Response:** Management confirmed that the Atlassian "standard – Change Management" was not reviewed timely as a formal policy refresh is currently ongoing. Formal updates and approval will be implemented at the time this refresh concludes.
		Atlassian has defined a Physical and Environmental Security policy which describes the guidelines for securing the building, offices, and equipment in detail. The policy is shared to all employee online and reviewed on an annual basis.
		Atlassian has defined a Backup policy which describes the framework for the development of procedures for the backup of resources in detail. The policy is shared to all employee online and reviewed on an annual basis.
		Atlassian has defined a Capacity Management policy which describes the structured capacity planning process ensuring Atlassian can meet customer and internal expectations for service, availability and reliability. The policy is shared to all employee online and reviewed on an annual basis.
		Atlassian has defined a Risk Assessment process document. The document is reviewed and approved on an annual basis.

Trust Service Criteria		Control Activities
		Atlassian employees are rewarded and recognised for their contribution and accomplishments as a part of their annual performance review process.
		Atlassian has defined a Policy Management Program (PMP) to ensure policies are reviewed at least annually by the designated policy owner or their delegate and are available online.
		Internal Audit performs audits on an annual basis. The results of internal audits are captured, and remediation is tracked with regular reports to management.

Trust Service Criteria		Control Activities
CC 6.1	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.	Atlassian has defined a Data Classification policy which describes the system of classification for operational use at Atlassian in detail. The policy is shared to all empl online and reviewed on an annual basis.
		Atlassian Focus maintains a data flow map for their systems and services that process personal data.
		A description of the system delineating the boundaries and describing relevant components of Atlassian focus is documented on the Atlassian intranet and the system features and functionality of Atlassian Focus is documented on the customer-facing Atlassian website.
		IT Asset Management software is used to monitor hard drive encryption, user authentication requirements and security patching on endpoint devices. **Exception Noted:** It was noted that the minimum endpoint baseline configuration for user authentication was not documented at the time of audit. **Management Response:** Management confirmed that the Atlassian “standard – Passwords” did not clearly outline configuration requirements specifically for endpoint devices. Management is updating this policy to explicitly include these requirements.
		A ZeroTrust infrastructure is implemented to place endpoints into a tiered network (High, Medium, Low, Open) based on their security posture and type of device. Applications added to the SSO platform are tiered according to the ZeroTrust policy. Endpoints cannot access applications via the SSO platform unless they are placed on the same/higher tier as the application.
		Two-factor authentication is required when launching an application from the Atlassian Identity User Portal.
		Active Directory enforces password settings in line with the Atlassian Password Standard.
		Atlassian has implemented two-factor authentication while logging into VPN.
		A malware protection system is implemented and enforced on all Atlassian corporate endpoints.

Trust Service Criteria		Control Activities
		Atlassian has enforced an authentication and authorization method to ensure all active cloud customers have a password that is, at minimum eight characters in length.
		Firewall rules are configured and maintained by the Micros Team. Changes to firewall rules require a peer reviewed pull request.
		External users connect to Jira using encrypted traffic via SSL protocol. Certificates are rotated when required.
		Access to the Atlassian internal network and internal tools is restricted to authorized users via logical access measures: i. Each user account must have an active AD (Active Directory) account. ii. Each user account must be a member of the appropriate AD group.
		Atlassian Micros Platform enforces encryption at rest for all services hosting User Generated Content (UGC).
		The Root user password for all AWS Management accounts meets password settings as defined in Standard - Passwords.
		External users connect to Atlassian Focus using encrypted traffic via TLS protocol. Certificates are rotated when required.
		Customer data stored by the Atlassian Focus product is logically partitioned through unique identifiers (activation IDs) separating the data from other customers.
		TDP maintains a data flow map for their systems and services that process personal data.
		TDP data is encrypted at-rest using AES-256 server-side encryption.
		Atlassian Focus data is encrypted at-rest using AES-256 server-side encryption.
CC 6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Access to customer data is supported by a valid customer support request or HOT ticket.
		Automatic provisioning and updating of AD role groups is performed via batch jobs which run in Orchestration. Active Directory contains a subset of groups which are automatically created and maintained based on demographic and employment information in Workday.
		Within 8 hours of a user account being marked as inactive in Workday, user accounts are suspended in Okta and Active Directory.
		Access to Atlassian Focus services is provisioned based on appropriate authorization by the service owner or delegate in SSAM.
		Atlassian performs privilege user access reviews for Atlassian Focus on a bi-annual basis **Exception Noted:** It was noted that for a selected Biannual Atlassian Focus User Access Review, the review was not performed completely and accurately, some user groups were left out from the scope of the review.

Trust Service Criteria		Control Activities
		Management Response: Management confirmed access to Atlassian Focus services were reviewed retroactively and confirmed appropriate. To prevent recurrence, Management is in the process of creating a centralized tool that will standardize audits and their respective user access levels.
		Access to Micros Platform is provisioned based on appropriate authorization by the service owner or delegate in SSAM.
		Atlassian performs privilege user access reviews for Micros Platform on a bi-annual basis. **Exception Noted:** It was noted that for a selected Biannual Micros User Access Review, the review was not performed completely and accurately, some user groups were left out from the scope of the review. **Management Response:** Management confirmed access to Micros services were reviewed retroactively and confirmed appropriate. To prevent recurrence, Management is in the process of creating a centralized tool that will standardize audits and their respective user access levels.
		Atlassian performs privilege user access reviews for Active Directory on a bi-annual basis.
		Atlassian performs privilege user access reviews for workday on a bi-annual basis. **Exception Noted:** It was noted that for a selected Workday privilege User Access Review, the review was not performed completely and accurately. Users having access to the generic accounts were not reviewed as a part of the review. **Management Response:** While a review of the generic accounts did occur, Management agrees that the review did not include users with access to the generic accounts with passwords. Management is updating process documentation to include these users in the generic account reviews moving forward.
		Only authorised service owners and delegates have the access to add, modify and remove user's access rights within SSAM containers.
		Access to assign delegates is restricted to container owner and the container delegates.
		Atlassian performs privilege user access reviews for SSAM containers on a bi-annual basis.
		Administrative access to SSAM is provisioned based on appropriate authorisation by the service owner or delegate.
		Organizational charts are updated based on employee transactions. Organizational charts are available to all Atlassian employees via Workday.

Trust Service Criteria		Control Activities
		The organizational charts are reviewed by appropriate Atlassian management and updated semi-annually.
		Atlassian has implemented two-factor authentication while logging into VPN.
		Privilege access to the Artifactory metadata in the Metadata Platform is restricted to the Metadata Collector services.
		Only docker images that exist in the Artifactory will be replicated to AWS ECR (Elastic Container Registry).
		In the event of a catastrophic failure, Atlassian workplace technology uses break glass procedures to bypass two factor authentication.
		Privileged access of Atlassian users to EC2 production environment is restricted to authorized and appropriate users only.
		Write access to production software artifacts in Artifactory is limited to the Development Tooling (Secrets and Artifacts), the automated build system, and Micros server.
		Access to TDP services is provisioned based on appropriate authorization by the service owner or delegate in SSAM.
		Atlassian performs privilege user access reviews for TDP on a bi-annual basis. **Exception Noted:** It was noted that for a selected Biannual TDP User Access Review, the review was not performed completely and accurately, some user groups were left out from the scope of the review. **Management Response:** Management confirmed access to TDP services were reviewed retroactively and confirmed appropriate. To prevent recurrence, Management is in the process of creating a centralized tool that will standardize audits and their respective user access levels.
		Access to the Atlassian internal network and internal tools is restricted to authorized users via logical access measures: i. Each user account must have an active AD (Active Directory) account. ii. Each user account must be a member of the appropriate AD group.
CC 6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation	Automatic provisioning and updating of AD role groups is performed via batch jobs which run in Orchestration. Active Directory contains a subset of groups which are automatically created and maintained based on demographic and employment information in Workday.
		Within 8 hours of a user account being marked as inactive in Workday, user accounts are suspended in Okta and Active Directory.
		Access to Atlassian Focus services is provisioned based on appropriate authorization by the service owner or delegate in SSAM.
		Atlassian performs privilege user access reviews for Atlassian Focus on a bi-annual basis.

Trust Service Criteria		Control Activities
	of duties, to meet the entity's objectives.	**Exception Noted:** It was noted that for a selected Biannual Atlassian Focus User Access Review, the review was not performed completely and accurately, some user groups were left out from the scope of the review. **Management Response:** Management confirmed access to Atlassian Focus services were reviewed retroactively and confirmed appropriate. To prevent recurrence, Management is in the process of creating a centralized tool that will standardize audits and their respective user access levels.
		Access to Micros Platform is provisioned based on appropriate authorization by the service owner or delegate in SSAM.
		Atlassian performs privilege user access reviews for Micros Platform on a bi-annual basis. **Exception Noted:** It was noted that for a selected Biannual Micros User Access Review, the review was not performed completely and accurately, some user groups were left out from the scope of the review. **Management Response:** Management confirmed access to Micros services were reviewed retroactively and confirmed appropriate. To prevent recurrence, Management is in the process of creating a centralized tool that will standardize audits and their respective user access levels.
		Atlassian performs privilege user access reviews for Active Directory on a bi-annual basis.
		Atlassian performs privilege user access reviews for workday on a bi-annual basis. **Exception Noted:** It was noted that for a selected Workday privilege User Access Review, the review was not performed completely and accurately. Users having access to the generic account were not reviewed as a part of the review. **Management Response:** While a review of the generic accounts did occur, Management agrees that the review did not include users with access to the generic accounts with passwords. Management is updating process documentation to include these users in the generic account reviews moving forward.
		Write access to production software artifacts in Artifactory is limited to the Development Tooling (Secrets and Artifacts), the automated build system, and Micros server.
		Privilege access to the Aartifactory metadata in the Metadata Platform is restricted to the Metadata Collector services.
		SSAM logs are read-only and direct access to the logs is restricted to the appropriate personnel.

Trust Service Criteria		Control Activities
		Only authorised service owners and delegates have the access to add, modify and remove user's access rights within SSAM containers.
		Access to assign delegates is restricted to container owner and the container delegates.
		Atlassian performs privilege user access reviews for SSAM containers on a bi-annual basis.
		Privileged access of Atlassian users to EC2 production environment is restricted to authorized and appropriate users only.
		Only docker images that exist in the Artifactory will be replicated to AWS ECR (Elastic Container Registry).
		In the event of a catastrophic failure, Atlassian workplace technology uses break glass procedures to bypass two factor authentication.
		Access to customer data is supported by a valid customer support request or HOT ticket.
		Access to the Atlassian internal network and internal tools is restricted to authorized users via logical access measures: i. Each user account must have an active AD (Active Directory) account. ii. Each user account must be a member of the appropriate AD group.
		Privileged access to Deployment Bamboo is restricted to the members of the Development Tooling team and the mobile CI stream within the mobile foundation team. **Exception Noted:** It was noted that access to Deployment Bamboo was not restricted to the authorized members as of 28 February 2025. We noted two users having privilege access to the Deployment Bamboo were not part of Development Tooling Team and the Mobile CI stream. **Management Response:** Due to an internal team reorganization, two individuals retained access longer than required. Access has since been removed and management has reviewed and reinforced our access control procedures to prevent further occurrences.
		An automatic alert is sent for any role change between the following groups: Engineering, Customer Support & Success (CSS), or Finance group. Appropriateness of access is reviewed and approved. **Exception Noted:** It was noted that for a selected user role change, appropriateness of access was not reviewed and approved timely. A delay of one month noted to complete the review. **Management Response:** Management identified and addressed the technical issues with the ticketing system to ensure role change tickets were reaching the responsible team. Management is refining the SLAs associated with process to ensure approvals are captured within a timely manner.

Trust Service Criteria		Control Activities
		Access to TDP services is provisioned based on appropriate authorization by the service owner or delegate in SSAM.
		Atlassian performs privilege user access reviews for TDP on a bi-annual basis. **Exception Noted:** It was noted that for a selected Biannual TDP User Access Review, the review was not performed completely and accurately, some user groups were left out from the scope of the review. **Management Response:** Management confirmed access to TDP services were reviewed retroactively and confirmed appropriate. To prevent recurrence, Management is in the process of creating a centralized tool that will standardize audits and their respective user access levels.
		Administrative access to SSAM is provisioned based on appropriate authorisation by the service owner or delegate.
CC 6.4	The entity restricts physical access to facilities and protected information assets (for example, data centre facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	The company's production environment is hosted at third-party data centres (AWS), which are carved out for the purposes of this report. Atlassian reviews SOC reports at least annually for material third party services and applications to ensure controls are appropriate and operating effectively as defined in Standard - Vendor Service Organisation Control (SOC) Report Review process document.
CC 6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	Cloud Provisioner listens for customer deletion requests and triggers deletion notifications. Cloud Provisioner has an automated retry mechanism to ensure requests are fulfilled. Failures are raised and tracked through the PROVFAIL Jira Project.
		Atlassian Focus customer data is retained as per the defined SLA. Data is deleted at the end of the retention period after the suspension of a client site.
		Within 8 hours of a user account being marked as inactive in Workday, user accounts are suspended in Okta and Active Directory.
		Atlassian has implemented secure disposal and re-use of equipment policy. Agreements are in place to manage procedures to sanitise, and wipe used Atlassian issued devices prior to repurposing.
		TDP customer data is retained as per the defined SLA. Data is deleted at the end of the retention period after the suspension of a client site.
		TDP production and non-production environments are segregated. Customer production data is not used in non-production environments.
		Atlassian Focus production and non-production environments are segregated. Customer production data is not used in non-production environments.

Trust Service Criteria		Control Activities
CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Atlassian Focus data is encrypted at-rest using AES-256 server-side encryption.
		IT Asset Management software is used to monitor hard drive encryption, user authentication requirements and security patching on endpoint devices. **Exception Noted:** It was noted that the minimum endpoint baseline configuration for user authentication was not documented at the time of audit. **Management Response:** Management confirmed that the Atlassian "standard – Passwords" did not clearly outline configuration requirements specifically for endpoint devices. Management is updating this policy to explicitly include these requirements.
		A ZeroTrust infrastructure is implemented to place endpoints into a tiered network (High, Medium, Low, Open) based on their security posture and type of device. Applications added to the SSO platform are tiered according to the ZeroTrust policy. Endpoints cannot access applications via the SSO platform unless they are placed on the same/higher tier as the application.
		Two-factor authentication is required when launching an application from the Atlassian Identity User Portal.
		Active Directory enforces password settings in line with the Atlassian Password Standard.
		A malware protection system is implemented and enforced on all Atlassian corporate endpoints.
		Firewall rules are configured and maintained by the Micros Team. Changes to firewall rules require a peer reviewed pull request.
		External users connect to Jira using encrypted traffic via SSL protocol. Certificates are rotated when required.
		External users connect to Confluence using encrypted traffic via SSL protocol. Certificates are rotated when required.
		TDP data is encrypted at-rest using AES-256 server-side encryption.
		External users connect to Atlassian Focus using encrypted traffic via TLS protocol. Certificates are rotated when required.
		Atlassian has implemented two-factor authentication while logging into VPN.
CC 6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to	Atlassian Focus data is encrypted at-rest using AES-256 server-side encryption.
		IT Asset Management software is used to monitor hard drive encryption, user authentication requirements and security patching on endpoint devices. **Exception Noted:** It was noted that the minimum endpoint baseline configuration for user authentication was not documented at the time of audit. **Management Response:**

Trust Service Criteria		Control Activities
	meet the entity's objectives.	Management confirmed that the Atlassian "standard – Passwords" did not clearly outline configuration requirements specifically for endpoint devices. Management is updating this policy to explicitly include these requirements.
		A ZeroTrust infrastructure is implemented to place endpoints into a tiered network (High, Medium, Low, Open) based on their security posture and type of device. Applications added to the SSO platform are tiered according to the ZeroTrust policy. Endpoints cannot access applications via the SSO platform unless they are placed on the same/higher tier as the application.
		Two-factor authentication is required when launching an application from the Atlassian Identity User Portal.
		Active Directory enforces password settings in line with the Atlassian Password Standard.
		A malware protection system is implemented and enforced on all Atlassian corporate endpoints.
		Firewall rules are configured and maintained by the Micros Team. Changes to firewall rules require a peer reviewed pull request.
		External users connect to Jira using encrypted traffic via SSL protocol. Certificates are rotated when required.
		Atlassian has implemented two-factor authentication while logging into VPN.
		USB mass storage devices are configured read-only for all Atlassian issued machines.
		External users connect to Confluence using encrypted traffic via SSL protocol. Certificates are rotated when required.
		TDP data is encrypted at-rest using AES-256 server-side encryption.
		External users connect to Atlassian Focus using encrypted traffic via TLS protocol. Certificates are rotated when required.
CC 6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Atlassian uses CrowdStrike to detect and prevent the installation of malicious software on endpoint devices. Upon detection of the chain of suspicious activities, a cyber ticket is created and assigned to the SecInt (Security Intelligence) team to review.
		Atlassian Perform review of logs to detect security events. Automated alerts are set up based on known and prior security events and incidents via Splunk. The Security Intelligence Team triages and investigates triggered alert. Incident Response Team investigates the true positive events and takes action as per the Incident Management process.
		Atlassian has defined a Change Management Policy which describes the process managing systems and services related changes in detail. The policy is shared to all employee online and reviewed on an annual basis. **Exception Noted:** It was noted that the policy document "standard – Change Management" was not reviewed by the designated policy owner.

Trust Service Criteria		Control Activities
		Management Response: Management confirmed that the Atlassian "standard – Change Management" was not reviewed timely as a formal policy refresh is currently ongoing. Formal updates and approval will be implemented at the time this refresh concludes.
		A malware protection system is implemented and enforced on all Atlassian corporate endpoints.

Trust Service Criteria		Control Activities
CC 7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify 1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Atlassian Perform review of logs to detect security events. Automated alerts are set up based on known and prior security events and incidents via Splunk. The Security Intelligence Team triages and investigates triggered alert. Incident Response Team investigates the true positive events and takes action as per the Incident Management process.
		A Jira ticket is automatically created in the REPCOM project upon alteration of the following settings related to the enforcement of peer review for in-scope code repositories in Bitbucket Cloud and Bitbucket Server: **Bitbucket Server:** i. Requires n approvers is unchecked in settings -> Pull Requests. ii. Unapprove automatically on new changes is unchecked in settings -> Pull requests. iii. Prevent changes without a pull request, except by is unchecked or users list is updated for a branch in settings -> Branch permissions **Bitbucket Cloud** i. If a branch is removed from the list enumerated in Enable SOX Compliance control on these branches. Note: Individual settings including the requirement of approvals and resetting of approvals when the source branch is modified cannot be altered without first removing the branch from this list. ii. If a user is granted "write access" to a branch which has SOX compliance enabled. The Jira ticket generated is automatically assigned to the direct manager of the person who initiated the change. The Assignee is responsible for: ii. Investigating the reason for the settings alteration and commenting on the ticket. iii. Confirming that the settings are re-enabled (if applicable). iv. Resolving the ticket after the settings have been re-enabled (if applicable) The REPCOM ticket must be completed/resolved within 3 weeks of being generated.
		Amazon API events are recorded via AWS CloudTrails and are read-only by policy. Alerts are reviewed and resolved within five business days, unless a more intensive follow-up is required.
		Penetration testing is performed by Atlassian using Bug Bounty on a continuous basis. The Vulnerabilities identified are tracked and resolved in accordance with the Vulnerability Management process document.

Trust Service Criteria		Control Activities
		Atlassian performs the container image scanning to identify vulnerable software in container images. Identified vulnerabilities are tracked and resolved in accordance with the Atlassian Vulnerability Management process document.
		Atlassian performs the software composition analysis to automatically scan code repositories for known vulnerabilities in third party dependencies. Identified vulnerabilities are tracked and resolved in accordance with the Atlassian Vulnerability Management process document.
		Atlassian performs the cloud configuration monitoring to scan AWS account configurations against a defined ruleset. Identified vulnerabilities are tracked and resolved in accordance with the Atlassian Vulnerability Management process document.
		Atlassian performs the host-based vulnerabilities to perform host-based scans of its infrastructure. Identified vulnerabilities are tracked and resolved in accordance with the Atlassian Vulnerability Management process document.
		TDP system vulnerability tickets are tracked and remediated to completion in a timely manner as per the vulnerability resolution standard.
		Atlassian Focus system vulnerability tickets are tracked and remediated to completion in a timely manner as per the vulnerability resolution standard.
CC 7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analysed to determine whether they represent security events.	Atlassian has defined an Incident Management Policy which describes the Incident Management process on how Atlassian responds to customer downtime or degraded service in detail. The policy is shared to all employee online and reviewed on an annual basis.
		Atlassian has defined a Security Incident Management Policy. The policy is shared to all employee online and reviewed on an annual basis.
		Incidents are recorded in the Incident Management Systems. For Major, Critical and Crisis Incidents (i.e., severity 2 and above), a Post Incident Review (PIR) is completed by SRE (Site Reliability Engineering) team.
		Atlassian performs the container image scanning to identify vulnerable software in container images. Identified vulnerabilities are tracked and resolved in accordance with the Atlassian Vulnerability Management process document.
		Atlassian performs the software composition analysis to automatically scan code repositories for known vulnerabilities in third party dependencies. Identified vulnerabilities are tracked and resolved in accordance with the Atlassian Vulnerability Management process document.
		Atlassian performs the cloud configuration monitoring to scan AWS account configurations against a defined ruleset. Identified vulnerabilities are tracked and resolved in accordance with the Atlassian Vulnerability Management process document.
		Atlassian performs the host-based vulnerabilities to perform host-based scans of its infrastructure. Identified vulnerabilities are tracked and resolved in accordance with the Atlassian Vulnerability Management process document.

Trust Service Criteria		Control Activities
		Penetration testing is performed by Atlassian using Bug Bounty on a continuous basis. The Vulnerabilities identified are tracked and resolved in accordance with the Vulnerability Management process document.
		Atlassian Perform review of logs to detect security events. Automated alerts are set up based on known and prior security events and incidents via Splunk. The Security Intelligence Team triages and investigates triggered alert. Incident Response Team investigates the true positive events and takes action as per the Incident Management process.
CC 7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Atlassian has defined an Incident Management Policy which describes the Incident Management process on how Atlassian responds to customer downtime or degraded service in detail. The policy is shared to all employee online and reviewed on an annual basis.
		Atlassian has defined a Security Incident Management Policy. The policy is shared to all employee online and reviewed on an annual basis.
		Atlassian Perform review of logs to detect security events. Automated alerts are set up based on known and prior security events and incidents via Splunk. The Security Intelligence Team triages and investigates triggered alert. Incident Response Team investigates the true positive events and takes action as per the Incident Management process.
		Atlassian uses CrowdStrike to detect and prevent the installation of malicious software on endpoint devices. Upon detection of the chain of suspicious activities, a cyber ticket is created and assigned to the SecInt (Security Intelligence) team to review.
		Incidents are recorded in the Incident Management Systems. For Major, Critical and Crisis Incidents (i.e., severity 2 and above), a Post Incident Review (PIR) is completed by SRE (Site Reliability Engineering) team.
CC 7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Atlassian has defined an Incident Management Policy which describes the Incident Management process on how Atlassian responds to customer downtime or degraded service in detail. The policy is shared to all employee online and reviewed on an annual basis.
		Atlassian Perform review of logs to detect security events. Automated alerts are set up based on known and prior security events and incidents via Splunk. The Security Intelligence Team triages and investigates triggered alert. Incident Response Team investigates the true positive events and takes action as per the Incident Management process.
		Atlassian uses CrowdStrike to detect and prevent the installation of malicious software on endpoint devices. Upon detection of the chain of suspicious activities, a cyber ticket is created and assigned to the SecInt (Security Intelligence) team to review.
		Internal or External users can report bugs, defects, or security, confidentiality and availability issues via Atlassian approved communication channels.
		Atlassian performs the software composition analysis to automatically scan code repositories for known vulnerabilities in third party dependencies. Identified

Trust Service Criteria		Control Activities
		vulnerabilities are tracked and resolved in accordance with the Atlassian Vulnerability Management process document.
		Atlassian performs the cloud configuration monitoring to scan AWS account configurations against a defined ruleset. Identified vulnerabilities are tracked and resolved in accordance with the Atlassian Vulnerability Management process document.
		Atlassian performs the host-based vulnerabilities to perform host-based scans of its infrastructure. Identified vulnerabilities are tracked and resolved in accordance with the Atlassian Vulnerability Management process document.
		Penetration testing is performed by Atlassian using Bug Bounty on a continuous basis. The Vulnerabilities identified are tracked and resolved in accordance with the Vulnerability Management process document.
		Incidents are recorded in the Incident Management Systems. For Major, Critical and Crisis Incidents (i.e., severity 2 and above), a Post Incident Review (PIR) is completed by SRE (Site Reliability Engineering) team.
CC 7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Atlassian has defined an Incident Management Policy which describes the Incident Management process on how Atlassian responds to customer downtime or degraded service in detail. The policy is shared to all employee online and reviewed on an annual basis.
		Atlassian has defined a Security Incident Management Policy. The policy is shared to all employee online and reviewed on an annual basis.
		Atlassian Perform review of logs to detect security events. Automated alerts are set up based on known and prior security events and incidents via Splunk. The Security Intelligence Team triages and investigates triggered alert. Incident Response Team investigates the true positive events and takes action as per the Incident Management process.
		PostgreSQL, RDS, Aurora, DynamoDB and AWS S3 Clumio media are backed up every hour. Backups are monitored for failures and remediated in a timely manner. Automated sample-based restoration testing is performed for PostgreSQL, RDS, Aurora and DynamoDB datastores according to the Restore Verification tool schedule. Restoration testing of AWS S3 is performed on at least an annual basis. Automated restorations are monitored for failures and remediated in a timely manner.
		A formal disaster recovery plan is in place for Micros which is reviewed and tested on a quarterly basis in accordance with the Atlassian BC/DR program. Micros completes a business impact analysis on a periodic basis to identify recovery objectives and classify Micros services.
		Incidents are recorded in the Incident Management Systems. For Major, Critical and Crisis Incidents (i.e., severity 2 and above), a Post Incident Review (PIR) is completed by SRE (Site Reliability Engineering) team.

Trust Service Criteria		Control Activities
		A formal disaster recovery plan is in place for Atlassian Focus systems which is reviewed and tested on a quarterly basis in accordance with the Atlassian BC/DR (Business Continuity/Disaster Recovery) program. Atlassian Focus teams completes a business impact analysis on a periodic basis to identify recovery objectives and classify services.
		A formal disaster recovery plan is in place for TDP systems which is reviewed and tested on a quarterly basis in accordance with the Atlassian BC/DR (Business Continuity/Disaster Recovery) program. TDP teams completes a business impact analysis on a periodic basis to identify recovery objectives and classify services.
		Internal or External users can report bugs, defects, or security, confidentiality and availability issues via Atlassian approved communication channels.

Trust Service Criteria		Control Activities
CC 8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Atlassian has defined a Change Management Policy which describes the process managing systems and services related changes in detail. The policy is shared to all employee online and reviewed on an annual basis. **Exception Noted:** It was noted that the policy document "standard – Change Management" was not reviewed by the designated policy owner. **Management Response:** Management confirmed that the Atlassian "standard – Change Management" was not reviewed timely as a formal policy refresh is currently ongoing. Formal updates and approval will be implemented at the time this refresh concludes.
		The Micros platform will not allow code artefacts to deploy or run on the platform unless they have been peer reviewed and have passed green build testing.
		Atlassian Focus changes are peer reviewed and pass the green build testing prior to production deployment.
		Tokenator performs a check when building code designed for deployment to the SOX namespace in Artifactory and only issues tokens for compliant builds. Compliant builds occur from a branch that enforces the following branch permissions settings in Bitbucket Cloud: i. Check for at least 1 approval ii. Approvals are reset when the source branch is modified Any changes to the code/functionality of Tokenator will undergo the standard PRGB (Peer Review and Green Build) process.
		The PRGB (Peer Review and Green Build) process enforced by Bitbucket does not allow production releases where pull request requester = pull request approver.
		Bamboo will not allow code to be deployed unless it has passed green build testing.

Trust Service Criteria		Control Activities
		Bitbucket Pipeline will not allow code to be deployed unless it has passed green build testing.
		Only docker images that exist in the Artifactory will be replicated to AWS ECR (Elastic Container Registry).
		Metadata Platform performs a check to validate that deployments are compliant as per the following repository settings on the deployment's source repositories: i. Requires >=1 approver. ii. Unapprove automatically on new changes. iii. Changes without a pull request If the deployment is not considered compliant, the deployment is rejected.
		Privileged access to Deployment Bamboo is restricted to the members of the Development Tooling team and the mobile CI stream within the mobile foundation team. **Exception Noted:** It was noted that access to Deployment Bamboo was not restricted to the authorized members as of 28 February 2025. We noted two users having privilege access to the Deployment Bamboo were not part of Development Tooling Team and the Mobile CI stream. **Management Response:** Due to an internal team reorganization, two individuals retained access longer than required. Access has since been removed and management has reviewed and reinforced our access control procedures to prevent further occurrences.
		Privilege access to the Artifactory metadata in the Metadata Platform is restricted to the Metadata Collector services.
		Write access to production software artifacts in Artifactory is limited to the Development Tooling (Secrets and Artifacts), the automated build system, and Micros server.
		Deployment Bamboo performs a check to validate that the following Bitbucket Server and Bitbucket Cloud SOX setting are enforced on the repositories: i. Requires >=1 approver. ii. Unapprove automatically on new changes. iii. Changes without a pull request If the following settings are not enforced, the code is rejected.
		TDP changes are peer reviewed and pass the green build testing prior to production deployment.
		A Jira ticket is automatically created in the REPCOM project upon alteration of the following settings related to the enforcement of peer review for in-scope code repositories in Bitbucket Cloud and Bitbucket Server: **Bitbucket Server:** i. Requires n approvers is unchecked in settings -> Pull Requests. ii. Unapprove automatically on new changes is unchecked in settings -> Pull requests.

Trust Service Criteria		Control Activities
		iii. Prevent changes without a pull request, except by is unchecked or users list is updated for a branch in settings -> Branch permissions **Bitbucket Cloud** i. If a branch is removed from the list enumerated in Enable SOX Compliance control on these branches. Note: Individual settings including the requirement of approvals and resetting of approvals when the source branch is modified cannot be altered without first removing the branch from this list. ii. If a user is granted "write access" to a branch which has SOX compliance enabled. The Jira ticket generated is automatically assigned to the direct manager of the person who initiated the change. The Assignee is responsible for: i. Investigating the reason for the settings alteration and commenting on the ticket. ii. Confirming that the settings are re-enabled (if applicable). iii. Resolving the ticket after the settings have been re-enabled (if applicable) The REPCOM ticket must be completed/resolved within 3 weeks of being generated.

Trust Service Criteria		Control Activities
CC 9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Atlassian has defined a Risk Assessment process document. The document is reviewed and approved on an annual basis.
		Atlassian develops and documents action plans associated with Enterprise Risks. Risk reviews are performed as per Atlassian Enterprise Risk Management capability document. **Exception Noted:** It was noted that for a selected risk, risk treatment plan and risk review were not performed in line with the Atlassian Enterprise Risk Management Policy. **Management Response:** Management identified the selected risk did not require a risk treatment plan as it should have been moved to an archived state. Management is in the process of migrating to a new risk tracking system as part of GRC tooling uplift that will enhance our risk management processes.
		A formal disaster recovery plan is in place for Micros which is reviewed and tested on a quarterly basis in accordance with the Atlassian BC/DR program. Micros completes a business impact analysis on a periodic basis to identify recovery objectives and classify Micros services.
		A formal disaster recovery plan is in place for Atlassian Focus systems which is reviewed and tested on a quarterly basis in accordance with the Atlassian BC/DR (Business Continuity/Disaster Recovery) program. Atlassian Focus teams completes a business impact analysis on a periodic basis to identify recovery objectives and classify services.

Trust Service Criteria		Control Activities
		Atlassian Internal Audit team prepares the results of the financial statement risk assessment and shares with the Head of Finance and Accounting for validation on an annual basis.
		A formal disaster recovery plan is in place for TDP systems which is reviewed and tested on a quarterly basis in accordance with the Atlassian BC/DR (Business Continuity/Disaster Recovery) program. TDP teams completes a business impact analysis on a periodic basis to identify recovery objectives and classify services.
		Atlassian has defined an Incident Management Policy which describes the Incident Management process on how Atlassian responds to customer downtime or degraded service in detail. The policy is shared to all employee online and reviewed on an annual basis.
CC 9.2	The entity assesses and manages risks associated with vendors and business partners.	Atlassian has defined a procurement policy which describes the vendor management process in detail. The policy is shared to all employee online and reviewed on an annual basis.
		Atlassian develops and documents action plans associated with Enterprise Risks. Risk reviews are performed as per Atlassian Enterprise Risk Management capability document. **Exception Noted:** It was noted that for a selected risk, risk treatment plan and risk review were not performed in line with the Atlassian Enterprise Risk Management Policy. **Management Response:** Management identified the selected risk did not require a risk treatment plan as it should have been moved to an archived state. Management is in the process of migrating to a new risk tracking system as part of GRC tooling uplift that will enhance our risk management processes.
		Employees and contractors are required to sign CIIAs (Confidential Information and Inventions Assignment) as part of the onboarding process.
		Atlassian reviews SOC reports at least annually for material third party services and applications to ensure controls are appropriate and operating effectively as defined in Standard - Vendor Service Organisation Control (SOC) Report Review process document.
		Based on the data shared with the third party, Atlassian third party contract outlines the required security and privacy controls.
		Atlassian signs agreement with the third-party outlining process of notifying of any breaches or information security incidents impacting the personal data stored by Atlassian.
		Atlassian communicates changes to confidentiality commitments through Atlassian's web site.
		Vendors and associated security, availability and confidentiality commitments are reviewed by appropriate Atlassian management during the procurement process and on an ongoing basis, as applicable.

Trust Service Criteria		Control Activities
		Exception Noted: It was noted that for a sample vendor, while a contract termination request process exists and is documented, a comprehensive vendor off-boarding process is not currently established and tracked via tickets. **Management Response:** Management is formalizing a comprehensive process to track the off boarding of vendors.

Trust Service Criteria		Control Activities
A 1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	Atlassian has defined a Capacity Management policy which describes the structured capacity planning process ensuring Atlassian can meet customer and internal expectations for service, availability and reliability. The policy is shared to all employee online and reviewed on an annual basis.
		Atlassian monitors changes to the TDP services availability and processing capacity. Alerts are triaged and resolved in a timely manner.
		Atlassian monitors changes to the Atlassian Focus services availability and processing capacity. Alerts are triaged and resolved in a timely manner.
A 1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	Atlassian has defined a Risk Assessment process document. The document is reviewed and approved on an annual basis.
		Atlassian develops and documents action plans associated with Enterprise Risks. Risk reviews are performed as per Atlassian Enterprise Risk Management capability document. **Exception Noted:** It was noted that for a selected risk, risk treatment plan and risk review were not performed in line with the Atlassian Enterprise Risk Management Policy. **Management Response:** Management identified the selected risk did not require a risk treatment plan as it should have been moved to an archived state. Management is in the process of migrating to a new risk tracking system as part of GRC tooling uplift that will enhance our risk management processes.
		Atlassian monitors changes to the Atlassian Focus services availability and processing capacity. Alerts are triaged and resolved in a timely manner.
		A formal disaster recovery plan is in place for Micros which is reviewed and tested on a quarterly basis in accordance with the Atlassian BC/DR (Business Continuity/Disaster Recovery) program. Micros completes a business impact analysis on a periodic basis to identify recovery objectives and classify Micros services.
		A formal disaster recovery plan is in place for Atlassian Focus systems which is reviewed and tested on a quarterly basis in accordance with the Atlassian BC/DR (Business Continuity/Disaster Recovery) program. Atlassian Focus teams completes a business impact analysis on a periodic basis to identify recovery objectives and classify services.
		Atlassian has defined a Backup policy which describes the framework for the development of procedures for the backup of resources in detail. The policy is shared to all employee online and reviewed on an annual basis.
		Atlassian reviews SOC reports at least annually for material third party services and applications to ensure controls are appropriate and operating effectively as defined in Standard - Vendor Service Organisation Control (SOC) Report Review process document.
		Changes to system availability is published externally to allow customers to check the status/uptime of Atlassian Focus in real-time.

Trust Service Criteria		Control Activities
		Atlassian monitors changes to the TDP services availability and processing capacity. Alerts are triaged and resolved in a timely manner.
		A formal disaster recovery plan is in place for TDP systems which is reviewed and tested on a quarterly basis in accordance with the Atlassian BC/DR (Business Continuity/Disaster Recovery) program. TDP teams completes a business impact analysis on a periodic basis to identify recovery objectives and classify services.
		PostgreSQL, RDS, Aurora, DynamoDB and AWS S3 Clumio media are backed up every hour. Backups are monitored for failures and remediated in a timely manner. Automated sample-based restoration testing is performed for PostgreSQL, RDS, Aurora and DynamoDB datastores according to the Restore Verification tool schedule. Restoration testing of AWS S3 is performed on at least an annual basis. Automated restorations are monitored for failures and remediated in a timely manner.
A 1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	A formal disaster recovery plan is in place for Micros which is reviewed and tested on a quarterly basis in accordance with the Atlassian BC/DR program. Micros completes a business impact analysis on a periodic basis to identify recovery objectives and classify Micros services.
		A formal disaster recovery plan is in place for Atlassian Focus systems which is reviewed and tested on a quarterly basis in accordance with the Atlassian BC/DR (Business Continuity/Disaster Recovery) program. Atlassian Focus teams completes a business impact analysis on a periodic basis to identify recovery objectives and classify services.
		A formal disaster recovery plan is in place for TDP systems which is reviewed and tested on a quarterly basis in accordance with the Atlassian BC/DR (Business Continuity/Disaster Recovery) program. TDP teams completes a business impact analysis on a periodic basis to identify recovery objectives and classify services.
		Atlassian has defined a Backup policy which describes the framework for the development of procedures for the backup of resources in detail. The policy is shared to all employee online and reviewed on an annual basis.
		PostgreSQL, RDS, Aurora, DynamoDB and AWS S3 Clumio media are backed up every hour. Backups are monitored for failures and remediated in a timely manner. Automated sample-based restoration testing is performed for PostgreSQL, RDS, Aurora and DynamoDB datastores according to the Restore Verification tool schedule. Restoration testing of AWS S3 is performed on at least an annual basis. Automated restorations are monitored for failures and remediated in a timely manner.

Trust Service Criteria		Control Activities
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Atlassian has defined a Data Classification policy which describes the system of data classification for operational use at Atlassian in detail. The policy is shared to all employee online and reviewed on an annual basis.
		Atlassian Focus production and non-production environments are segregated. Customer production data is not used in non-production environments.
		Vendors and associated security, availability and confidentiality commitments are reviewed by appropriate Atlassian management during the procurement process and on an ongoing basis, as applicable. **Exception Noted:** It was noted that for a sample vendor, while a contract termination request process exists and is documented, a comprehensive vendor off-boarding process is not currently established and tracked via tickets. **Management Response:** Management is formalizing a comprehensive process to track the off boarding of vendors.
		Atlassian communicates changes to confidentiality commitments through Atlassian's web site.
		Customer terms of service (ToS) are standardized and approved by legal. The ToS communicate Atlassian's security, availability and confidentiality commitments and the customer responsibilities and obligations. Any changes to these commitments or responsibilities in the ToS are communicated to customers pursuant to the notification procedures specified in the ToS.
		Cloud Provisioner listens for customer deletion requests and triggers deletion notifications. Cloud Provisioner has an automated retry mechanism to ensure requests are fulfilled. Failures are raised and tracked through the PROVFAIL Jira Project.
		Atlassian reviews SOC reports at least annually for material third party services and applications to ensure controls are appropriate and operating effectively as defined in Standard - Vendor Service Organisation Control (SOC) Report Review process document.
		TDP production and non-production environments are segregated. Customer production data is not used in non-production environments.
		Internal or External users can report bugs, defects, or security, confidentiality and availability issues via Atlassian approved communication channels.
C 1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	Atlassian's Policy mandates secure disposal of hard copy material. Secure bins are available in each Atlassian location for the disposal of information and contracts are in place with Shred-X to handle the secure destruction of hard copy material.
		Atlassian has implemented secure disposal and re-use of equipment policy. Agreements are in place to manage procedures to sanitise, and wipe used Atlassian issued devices prior to repurposing.
		Cloud Provisioner listens for customer deletion requests and triggers deletion notifications. Cloud Provisioner has an automated retry mechanism to ensure

Trust Service Criteria		Control Activities
		requests are fulfilled. Failures are raised and tracked through the PROVFAIL Jira Project.
		Vendors and associated security, availability and confidentiality commitments are reviewed by appropriate Atlassian management during the procurement process and on an ongoing basis, as applicable. **Exception Noted:** It was noted that for a sample vendor, while a contract termination request process exists and is documented, a comprehensive vendor off-boarding process is not currently established and tracked via tickets. **Management Response:** Management is formalizing a comprehensive process to track the off boarding of vendors.
		Atlassian reviews SOC reports at least annually for material third party services and applications to ensure controls are appropriate and operating effectively as defined in Standard - Vendor Service Organisation Control (SOC) Report Review process document.
		TDP customer data is retained as per the defined SLA. Data is deleted at the end of the retention period after the suspension of a client site.
		Atlassian Focus customer data is retained as per the defined SLA. Data is deleted at the end of the retention period after the suspension of a client site.

Annexure: List of Abbreviations:

No	Abbreviation	Expanded Form
1	2FA	2 Factor Authentication
2	AD	Active Directory
3	AES	Advanced Encryption Standard
4	AICPA	American Institute of Certified Public Accountants
5	ALB	Amazon Load Balancers
6	APC	Atlassian Policy Committee
7	API	Application Programming Interface
8	AWS	Amazon Web Services
9	AZ	Availability Zones
10	BC	Business Continuity
11	CIIA	Confidential Information and Inventions Assignment
12	COSO	The Committee of Sponsoring Organizations of the Treadway Commission
13	CSOC	Complementary Sub-Service Organization Controls
14	CSS	Customer Support & Success
15	CUEC	Complementary User Entity Controls
16	DR	Disaster Recovery
17	EC2	Amazon Elastic Compute Cloud
18	ECR	Elastic Container Registry
19	ERS	Entity Relationship Store
20	EU	European Union
21	FCPA	Foreign Corrupt Practices Act
22	HIPAA	Health Insurance Portability and Accountability Act
23	HTTPS	Hypertext Transfer Protocol Secure
24	IaaS	Infrastructure as a Service
25	iCIMS	Internet Collaborative Information Management Systems
26	IESBA	International Ethics Standards Board for Accountants
27	IP	Internet Protocol
28	IPO	Initial Public Offering

No	Abbreviation	Expanded Form
29	IR	Incident Response
30	ISO	International Organization for Standardization
31	IT	Information Technology
32	JSM	Jira Service Management
33	KMS	Key Management Services
34	MFA	Multi-Factor Authentication
35	NDA	Non-Disclosure Agreement
36	PIR	Post Incident Review
37	PITR	Point-In-Time Data Recovery
38	PRGB	Peer Review and Green Build
39	PROVFAIL	Provisioning Failure
40	R4	Rolling 4
41	REPCOM	Repository Compliance
42	RDS	Relational Database Service
43	RPO	Recovery Point Objective
44	RTO	Recovery Time Objective
45	S3	Amazon Simple Storage Service
46	SecInt	Security Intelligence
47	SLA	Service Level Agreement
48	SLO	Service Level Objective
49	SNS	Amazon Simple Notification Service
50	SoA	State of Atlassian
51	SOC	Service Organization Controls
52	SOP	Standard Operating Procedure
53	SSAM	Self Service Access Management
54	SSO	Single Sign-On
55	SQS	Amazon Simple Queue Service
56	SRE	Site Reliability Engineering
57	TA Ops	Talent Acquisition Operations
58	TDP	Transactional Data Platform

No	Abbreviation	Expanded Form
59	TLS	Transport Layer Security
60	ToS	Terms Of Service
61	TSP	Trust Services Principles
62	UAR	User Access Review
63	UGC	User Generated Content
64	VPC	Virtual Private Cloud
65	VPN	Virtual Private Network
66	WAF	Web Application Firewall