Report on Atlassian Corporation Plc's Description of Its Loom Product and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security, Availability, and Confidentiality Throughout the Period June 30, 2024 to September 30, 2024

SOC 2® - SOC for Service Organizations: Trust Services Criteria

Table of Contents

Section 1

Independent Service Auditor’s Report

Independent Service Auditor's Report

To: Atlassian Corporation Plc ("Atlassian")

Scope

We have examined Atlassian's accompanying description in Section 3 titled "Atlassian Corporation Plc's Description of Its Loom Product Throughout the Period June 30, 2024 to September 30, 2024" (description) based on the criteria for a description of a service organization's system set forth in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022*) (2018 description criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period June 30, 2024 to September 30, 2024, to provide reasonable assurance that Atlassian's 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 (With Revised Points of Focus—2022)* (2017 TSC).

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 examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Atlassian uses a subservice organization to provide data center colocation 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 examination 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 information included in Section 5, "Other Information Provided by Atlassian Corporation Plc That Is Not Covered by the Service Auditor's Report," is presented by Atlassian's management to provide additional information and is not a part of Atlassian's description of its Loom Product made available to user entities during the period June 30, 2024 to September 30, 2024. Information included in Atlassian's responses to testing exceptions has not been subjected to the procedures applied in the examination and, accordingly, we express no opinion on it.

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. In Section 2, Atlassian has provided the accompanying assertion titled "Assertion of Atlassian Corporation Plc Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated

therein. Atlassian is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; 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 the service organization'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 design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves—

- 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 or did not operate effectively.
- 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 achieved its service commitments and system requirements based on the applicable trust services criteria.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

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 individual report users may consider important to meet their informational needs. There are inherent limitations in 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 or operating effectiveness 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.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in Section 4, “Trust Services Criteria, Related Controls and Tests of Controls Relevant to the Security, Availability, and Confidentiality Categories” of this report.

Opinion

In our opinion, in all material respects—

a. The description presents Atlassian’s Loom Product that was designed and implemented throughout the period June 30, 2024 to September 30, 2024, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period June 30, 2024 to September 30, 2024, 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 throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Atlassian’s controls throughout that period.

c. The controls stated in the description operated effectively throughout the period June 30, 2024 to September 30, 2024, to provide reasonable assurance that Atlassian’s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Atlassian’s controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Atlassian, user entities of Atlassian’s Loom Product during some or all of the period June 30, 2024 to September 30, 2024, business partners of Atlassian subject to risks arising from interactions with Atlassian’s Loom Product, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators 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.

- 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. If a report recipient is not a specified party as defined above and has obtained this report, or has access to it, use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against Coalfire Controls, LLC as a result of such access. Further, Coalfire Controls, LLC does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Coalfire Controls LLC

Greenwood Village, Colorado
November 25, 2024

Section 2

Assertion of Atlassian Corporation Plc Management

Assertion of Atlassian Corporation Plc ("Atlassian") Management

We have prepared the accompanying description in Section 3 titled "Atlassian Corporation Plc's Description of Its Loom Product Throughout the Period June 30, 2024 to September 30, 2024" (description), based on the criteria for a description of a service organization's system set forth in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022*) (2018 description criteria). The description is intended to provide report users with information about the Loom Product 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 (With Revised Points of Focus—2022)* (2017 TSC).

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.

Atlassian uses a subservice organization for data center colocation 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.

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

a. The description presents Atlassian's Loom Product that was designed and implemented throughout the period June 30, 2024 to September 30, 2024, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period June 30, 2024 to September 30, 2024, 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 throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Atlassian's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period June 30, 2024 to September 30, 2024, to provide reasonable assurance that Atlassian's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Atlassian's controls operated effectively throughout that period.

Vikram Rao
Chief Trust Officer
Atlassian Corporation Plc

Section 3

Atlassian Corporation Plc's Description of Its Loom Product Throughout the Period June 30, 2024 to September 30, 2024

Type of Services Provided

Company Overview and Background

Atlassian Corporation Plc (“Atlassian” or “the Company”) was established in 2002 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 in the United States (San Francisco, Mountain View, New York City, Austin, Seattle), Australia (Sydney), the Philippines (Manila), Japan (Yokohama), the Netherlands (Amsterdam), Poland (Gdansk), Turkey (Ankara), and India (Bengaluru).

Atlassian's 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 collaborate and deliver quality results on time.

Overview of Products and Features

Loom

Loom is a video messaging tool that allows users to easily record through their camera, microphone, and desktop simultaneously. Loom videos are instantly sharable after recording with the click of a button.

The system description in this section of the report details the Atlassian product described above. Any other Company product or features are not within the scope of this report. The accompanying description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at any subservice organizations (see below for further discussion of the subservice organization).

Principal Service Commitments and System Requirements

Atlassian designs its processes and procedures to align with the objectives of Loom. These objectives are formulated according to the service commitments made by Atlassian to user entities; the laws and regulations governing the provision of the Loom System; and the financial, operational, and compliance requirements that Atlassian has established for the Systems.

The commitments to user entities regarding security, availability, and confidentiality are documented and communicated through various channels, such as the Atlassian Customer Agreement, Product-Specific Terms of Services, Data Processing Addendums, the sign-up page, the Privacy Policy, and the Atlassian Trust Center. The commitments to security, availability, and confidentiality include, but are not limited to, the following.

Trust Services Category	Service Commitments
Security	• Atlassian will implement and maintain physical, technical, and administrative security measures designed to protect customer data from unauthorized access, destruction, use, modification, or disclosure. • Atlassian will maintain a compliance program that includes independent third-party audits and certifications. • Upon becoming aware of a security incident, Atlassian will notify customers without undue delay.

Trust Services Category	Service Commitments
Availability	• Atlassian will use commercially reasonable efforts to maintain the availability of the products.
Confidentiality	• Atlassian will not disclose confidential information to any third party unless they have a business need to know. • Atlassian will not use confidential information for any purpose other than providing the services. • Upon termination of the services, Atlassian will delete or return customer data in accordance with the retention periods.

Atlassian establishes operational requirements that support the achievement of its security, availability, and confidentiality commitments, as well as relevant laws and regulations and other system requirements. These requirements are communicated through Atlassian's system policies and procedures, system design documentation, and contracts with customers. Atlassian's information security policies define an organization-wide approach to protecting systems and data. These policies include those related to the design and development of services, operation of the system, management of internal business systems and networks, and employee hiring and training. Standard operating procedures have been documented for carrying out specific manual and automated processes required for the operation and development of Loom.

Atlassian System Components

The boundaries of Loom refer to the aspects of the company's infrastructure, software, personnel, procedures, and data that are essential for providing its products and that directly contribute to the products offered to customers. The sections below provide a description of the components that directly support the products offered to customers. Any infrastructure, software, personnel, procedures, or data that provide support indirectly are not included.

Infrastructure

Atlassian products and features utilize Amazon Web Services (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.

The Loom Product is deployed to the AWS U.S. West region 2.

Network

Atlassian has public ingress points in the U.S. AWS region. These ingress points are behind Amazon CloudFront for Loom. All traffic from the internet is over Transport Layer Security (TLS), and TLS termination happens at Amazon CloudFront. 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 Loom 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 generate notifications and are tracked internally so that the certificates 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.

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 Loom Infrastructure 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.

Database

The Product utilizes a multi-tenant environment where the data is segregated by tenant using a unique identifier to query customer data. Unique cloud IDs do not share any common data to ensure segregation between customers.

The databases implemented by Loom operate in multiple availability zones (AZs) within the same region to mitigate the risk of data loss due to hardware failure. The datastores used by Loom consist of Amazon Relational Database Service (Amazon RDS) clusters located within the private network hosted in AWS and Amazon Simple Storage Service (Amazon S3).

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

Software

The following table lists the software, services and tools that support the control environment of Loom:

Function	Name
Hosting Systems	• Amazon Elastic Compute Cloud (Amazon EC2) • Amazon Elastic Kubernetes Service (Amazon EKS)
Storage and Database	• Amazon RDS • Amazon S3
Network	• Amazon VPC • Application Load Balancers (ALB) • Amazon CloudFront • AWS Web Application Firewall (WAF)
Application Cache	• Amazon ElastiCache
Encryption	• Amazon Key Management Service (AWS KMS) • AWS Secrets Manager
Search and Analytics	• Amazon OpenSearch Service • Google Tag Manager • Segment

Function	Name
Messaging	• Amazon Simple Notification Service (Amazon SNS) • Amazon Simple Queue Service (Amazon SQS) • CloudAMQP
Build, Release, and Continuous Integration Systems	• Argo CD • CircleCI • GitHub • LaunchDarkly • Terraform
Access Management	• Active Directory (AD) • CyberArk Idaptive single sign-on (SSO) • Duo two-factor authentication (2FA) • Okta SSO • Idaptive SSO • 1Password
Monitoring and Alerting	• AWS CloudTrail • Amazon CloudWatch • Amazon GuardDuty • Datadog • Panther • Sentry • Splunk
Certificate Management	• AWS Certificate Manager
Customer Support and Communication	• Zendesk
Vulnerability Scanning	• HackerOne • CrowdStrike • Snyk • Tenable
Human Resources (HR)	• Datapeople • Elevate • iCIMS • Recruitment Central • Workday

Function	Name
Learning, Training, and Development	• Absorb • Get Abstract • Haekka • Intellum • Learndot • Learning Central • LinkedIn Learning
Asset Management	• BitLocker • FileVault • Jamf Pro • Workspace One

AWS provides physical and environmental safeguards, infrastructure support, management, and storage services. Atlassian has identified the complementary subservice organization controls of AWS to achieve the applicable Trust Services Criteria.

The other third-party vendors mentioned above are only applicable to support specific controls.

People

The Company develops, manages, and secures Loom 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, confidentiality, product counsel, general counsel operations, and public relations
Engineering	Responsible for the development, testing, deployment, and maintenance of new code for the Atlassian products and features
Trust	Responsible for the management of access controls, the security of the production environment, enterprise risk management, business continuity, and compliance for the Atlassian products and features
Platform and Enterprise Cloud	Responsible for architecting, building, and maintaining the Atlassian products and features

People	
Group/Role Name	**Function**
Ecosystem	Responsible for third-party connectivity platforms and applications
Foundation	Responsible for harnessing the resources of Atlassian to champion organizations who believe that education is the key to eliminating disadvantage
Product	Responsible for overseeing the product lifecycle, including adding new product functionality

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

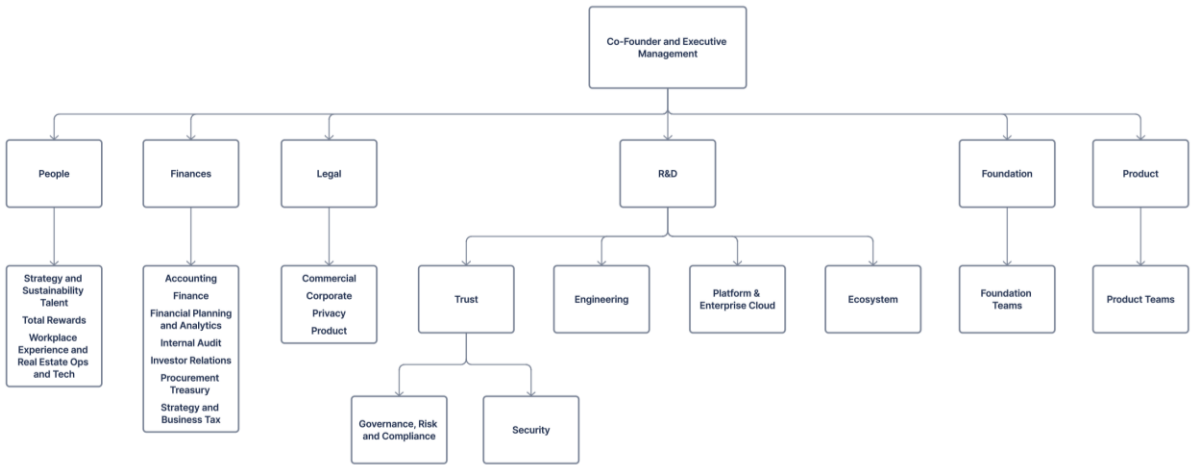

Figure 1: Atlassian Organizational Chart

Policies and Procedures

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

- Are properly communicated throughout the organization
- Are properly owned, managed, and supported
- Clearly outline business objectives
- Show commitment to meeting regulatory obligations
- Are focused on continual iteration and improvement
- Provide for an exception process
- Are supported by the Policy Framework and Structure

Atlassian defines policies, standards, guidelines, and procedures. 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 procedure-specific requirements that must be met by all personnel.
Guideline	Common practice recommendations and suggestions	Collection of system-specific or procedure-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, 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 achieve a consistent outcome defined by the standard or guideline.

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 the Executive Management team. Policy owners can approve exceptions for a period of no longer than one year.

Policy Review Process

For a policy, standard, guideline, or standard operating procedure to be 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 APC, 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 labeled to manage appropriate handling.
- All removable media should be managed with the same handling guidelines, as described 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
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 customers if mishandled	• Confidential personal data elements • Information related to business plans or deals • Information under a nondisclosure 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

System Incidents

There were no identified significant system incidents that (a) were the result of controls that were not suitably designed or operating effectively to achieve one or more of the service commitments and system requirements or (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements from June 30, 2024 to September 30, 2024.

The Applicable Trust Services Criteria and Related Controls

Applicable Trust Services Criteria

The Trust Services Categories that are in scope for the purposes of this report are as follows:

- *Security*: Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise availability or confidentiality of the information or systems and affect the entity's ability to meet its objectives.
- *Availability:* Information and systems are available for operation and use to meet the entity's objectives.
- *Confidentiality*: Information designated as confidential is protected to meet the entity's objectives.

Many of the criteria used to evaluate a system are shared amongst all in-scope categories; for example, the criteria related to risk assessment apply to the security, availability, and confidentiality categories. As a result, the criteria for the security, availability, and confidentiality categories are organized into (a) the criteria that are applicable to all categories (common criteria) and (b) criteria applicable only to a single category. The common criteria constitute the complete set of criteria for the security category. For the categories of availability and confidentiality, a complete set of criteria is comprised of all the common criteria and all the criteria applicable to the category being reported on.

The common criteria are organized as follows:

1. *Control environment:* The criteria relevant to how the entity is structured and the processes the entity has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values, qualifications of personnel, and the environment in which they function.
2. *Information and communication:* The criteria relevant to how the entity communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.
3. *Risk assessment:* The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.
4. *Monitoring activities:* The criteria relevant to how the entity monitors the system, including the suitability and design and operating effectiveness of the controls, and acts to address deficiencies identified.
5. *Control activities:* The criteria relevant to 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.
6. *Logical and physical access controls:* The criteria relevant to how the entity restricts logical and physical access, provides and removes that access, and prevents unauthorized access.
7. *System operations:* The criteria relevant to how the entity manages the operation of system(s) and detects and mitigates processing deviations, including logical and physical security deviations.
8. *Change management:* The criteria relevant to how the entity identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.

9. *Risk mitigation:* The criteria relevant to how the entity identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

This report is focused solely on the security, availability, and confidentiality categories. The Company has elected to exclude the processing integrity and privacy categories.

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. 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 the Financial Expert role, the meeting calendar, and the agenda, which is developed annually with results published after each meeting.

Board and Governance Committee Charter

The Board of Directors and its subcommittees (Audit, Nominating and Governance, and 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 Management 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 Behavior

Atlassian requires all employees and specified contractors to acknowledge the Code of Business Conduct and Ethics, 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 Code of Business Conduct and Ethics policy is reviewed annually. 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 and Ethics, 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 Confidential Information and Inventions Assignment (CIIA) 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.

Information and Communication

Internal Audit

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

Awareness and Training

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

Program Management

Atlassian maintains 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 at least semiannually.

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 the 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 annually. 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.

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 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 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, and 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

Vulnerability Management

Atlassian performs continuous vulnerability scanning. Atlassian ensures that any legitimate vulnerabilities are remediated in accordance with the vulnerability management policy.

Penetration Testing

Atlassian conducts penetration testing at least annually 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.

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. Atlassian has implemented role-based security to limit and control access within Loom’s production environment as defined in an access matrix. Additional access outside of the access matrix is provisioned in line with the principle of least privilege only after approval is documented.

Access to the Loom environment is revoked within three business days of a user’s termination.

Quarterly, a user access review of accounts in the system, including privileged, shared, generic, and bot accounts, is performed.

Identification and Authentication

Atlassian products and features are secured with passwords and multifactor 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 Atlassian password standard. Atlassian's SSO portals (Idaptive and Okta) allow 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.

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

System Operations

Boundary Protection

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 changes to products, features, and infrastructure are tested, reviewed, approved, and documented. Change management responsibilities are segregated among designated personnel. Emergency changes require retroactive review and approval within three business days. Configuration changes are documented and monitored for non-compliance. An alert is automatically generated and acknowledged by the Loom Security team if a branch protection rule relating to review and approval requirements is overridden.

Prevention of Unauthorized Changes

Information technology (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

Loom has a 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 (RTO)/recovery point objective (RPO), roles and responsibilities.

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 at least daily and annual 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.

Confidentiality

Information Handling and Retention

Following the receipt of a request for deletion of data from a customer, Loom customer data is deleted within 30 days and retained in backups for 30 days following the deletion.

Access to Customer Data

Customer data is logically isolated through the use of unique identifiers. Access to customer data requires customer consent before accessing.

Complementary User Entity Controls (CUECs)

The Company's controls related to Loom cover only a portion of overall internal control for each user entity. It is not feasible for the service commitments, system requirements, and applicable criteria related to the system to be achieved solely by the Company. Therefore, each user entity's internal control should be evaluated in conjunction with the Company's controls and the related tests and results described in Section 4 of this report, considering the related CUECs identified for the specific criterion. 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.

Criteria	Complementary User Entity Controls
CC6.1	• User entities are responsible for configuring their own instance, including the appropriate setup 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 characters where they have migrated from another identity service. • User entities are responsible for the safeguarding of their own account access credentials.
CC6.6 CC6.8 C1.1 C1.2	• User entities are responsible for security, including virus scans and the confidentiality of the data being 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 CC6.3 C1.2	• User entities are responsible for requesting removal of their account.
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.

Subservice Organizations and Complementary Subservice Organization Controls (CSOCs)

The Company uses AWS as a subservice organization for data center colocation services. The Company's controls related to Loom cover only a portion of the overall internal control for each user entity of Loom. The description does not extend to the colocation services for IT infrastructure provided by the subservice organization. Section 4 of this report and the description of the system only cover 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's physical security controls should mitigate the risk of unauthorized access to the hosting facilities. AWS's 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 Loom to be achieved solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls and related tests and results described in Section 4 of this report, considering the related CSOCs expected to be implemented at AWS as described below.

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

Specific Criteria Not Relevant to the System

There were no specific security, availability, or confidentiality Trust Services Criteria as set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy (With Revised Points of Focus—2022)* (2017 TSC) that were not relevant to the system as presented in this report.

Significant Changes to the System

Atlassian is in the process of a phased migration from Idaptive to Okta beginning in July 2024. The migration had not been completed as of September 30, 2024.

There were no other changes that are likely to affect report users' understanding of how Loom was used to provide the service from June 30, 2024 to September 30, 2024.

Report Use

The description does not omit or distort information relevant to Loom while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to their own needs.

Section 4

Trust Services Criteria, Related Controls and Tests of Controls Relevant to the Security, Availability, and Confidentiality Categories

Control Environment Elements

The control environment represents the collective effect of various elements in establishing, enhancing or mitigating the effectiveness of specific controls. The control environment elements as described in the description of the system include, but are not limited to, the Code of Business Conduct and Ethics, Policies and Procedures and Human Resources.

Our tests of the control environment included the following procedures, to the extent we considered necessary; (a) an inspection of Atlassian's organizational structure including segregation of functional responsibilities and policies and procedures; (b) inquiries with management, operations, administrative and other personnel who are responsible for developing, ensuring adherence to and applying controls; (c) observations of personnel in the performance of their assigned duties; and (d) inspection of documents and records pertaining to controls.

Description of Tests Performed by Coalfire Controls, LLC

Our tests of operating effectiveness of controls included such tests as were considered necessary in the circumstances to evaluate whether those controls, and the extent of compliance with them, were sufficient to provide reasonable, but not absolute, assurance that the trust services security, availability, and confidentiality categories and criteria were achieved throughout the period June 30, 2024 to September 30, 2024. In selecting particular tests of the operating effectiveness of the controls, we considered (i) the nature of the controls being tested; (ii) the types of available evidential matter; (iii) the nature of the criteria to be achieved; (iv) the assessed level of control risk; and (v) the expected efficiency and effectiveness of the test. Such tests were used to evaluate fairness of the presentation of the description of Atlassian's Loom Product and to evaluate the operating effectiveness of specified controls.

Additionally, observation and inspection procedures were performed as it relates to system generated reports, queries, and listings within management's description of the system to assess the completeness and accuracy (reliability) of the information utilized in the performance of our testing of the control activities.

Trust Services Criteria, Related Controls and Tests of Controls Relevant to the Security, Availability, and Confidentiality Categories

Control Environment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC1.1	The entity demonstrates a commitment to integrity and ethical values.		
	A comprehensive Code of Business Conduct and Ethics policy describes employee and contractor responsibilities and expected behavior regarding data and information system usage. The policy is shared with employees and reviewed annually.	Inspected the Code of Business Conduct and Ethics policy available internally via the Company intranet to determine that the policy was in place to describe employee and contractor responsibilities and expected behavior regarding data and information system usage, was shared with employees, and was reviewed according to its regular cadence.	No exceptions noted. The policy was reviewed during its normal cadence in December 2023.
	Employees acknowledge the Code of Business Conduct and Ethics policy upon hire.	Inspected acknowledgements for a sample of new employees to determine that new employees acknowledged that they had read and agreed to the Code of Business Conduct and Ethics policy upon hire.	Exception noted. 2 out of a sample of 12 new employees did not acknowledge the Code of Business Conduct and Ethics policy upon hire.
	Employee performance is reviewed annually.	Inspected performance appraisal documentation for a sample of employees to determine that performance appraisals were completed during the period.	No exceptions noted.
	The Company has documented disciplinary actions in a formalized sanctions policy for employees and contractors who violate the Code of Business Conduct and Ethics.	Inspected the Code of Business Conduct and Ethics to determine that the Company had documented disciplinary actions in a formalized sanctions policy for employees and contractors who violated the Code of Business Conduct and Ethics.	No exceptions noted.

Control Environment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Background checks are performed prior to an employee's start date in compliance with local laws and regulations.	Inspected background check completion evidence for a sample of new employees to determine that background checks were performed prior to their start date in compliance with local laws and regulations.	No exceptions noted.
	Employees and contractors are required to sign Confidential Information and Inventions Assignments (CIIAs) as part of the onboarding process.	Inspected signed CIIAs for a sample of new employees and contractors to determine that CIIAs were signed as part of the onboarding process.	No exceptions noted.
	A weekly review is performed to determine that the CIIA and background checks are completed for new employees as part of onboarding procedures.	Inspected weekly reviews for a sample of weeks to determine that a weekly review was performed to confirm that CIIAs and background checks were completed for new employees as part of onboarding procedures.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.		
	The Board and Committee Charter outlines the roles, responsibilities, and key activities of the board.	Inspected the Board and Committee Charter and meetings to determine that the roles, responsibilities, and key activities of the board were outlined.	No exceptions noted.
	The Audit Committee Charter outlines the roles, responsibilities, and key activities of the Audit Committee.	Inspected the Audit Committee Charter to determine that the roles, responsibilities, and key activities of the Audit Committee were documented.	No exceptions noted.

Control Environment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	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.	Inspected meeting minutes to determine that the Board of Directors and its subcommittees met during the period to review committee charters, corporate governance, and strategic operational objectives, and that meeting minutes included details on participants and dates.	No exceptions noted.
	The Governance Committee Charter outlines the roles, responsibilities, and key activities of the Governance Committee.	Inspected the Governance Committee Charter to determine that it outlined the roles, responsibilities, and key activities of the Governance Committee.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		
	An organizational chart is in place and updated to ensure identification of roles and responsibilities. The chart is reviewed and updated at least semiannually.	Inspected the organization chart and review documentation to determine that an organizational chart was in place and updated to ensure identification of roles and responsibilities and was reviewed and updated during its regular cadence.	No exceptions noted. The organization chart was reviewed and updated during its normal cadence in April 2024.
	Management has established defined roles and responsibilities to oversee the implementation of the security and control environment.	Inspected the Atlassian Security Policy to determine that management had established defined roles and responsibilities to oversee the implementation of the security and control environment.	No exceptions noted.
	The hiring manager reviews and approves employee job descriptions.	Inspected system workflows and templates to determine that job descriptions were reviewed and approved by the hiring manager and included authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	No exceptions noted.

Control Environment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
	Employees are required to complete security awareness training at least annually.	Inspected training completion evidence for a sample of employees to determine that employees were required to complete security awareness training during the period.	Exceptions noted. 2 out of a sample of 44 employees did not complete the required security awareness training during the period.
	During on-boarding, new employees are delivered security awareness training to introduce them to where to find resources and minimum standards and where to ask questions.	Inspected training completion evidence for a sample of new employees to determine that new employees were delivered security awareness training during onboarding to introduce them to where to find resources and minimum standards and where to ask questions.	No exceptions noted.
	A personnel development program for security and confidentiality has been established.	Inspected training tools made available to all employees to determine that a personnel development program for security and confidentiality had been established.	No exceptions noted.
	The hiring manager reviews and approves employee job descriptions.	Inspected system workflows and templates to determine that job descriptions were reviewed and approved by the hiring manager and included authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	No exceptions noted.
	Employee performance is reviewed annually.	Inspected performance appraisal documentation for a sample of employees to determine that performance appraisals were completed during the period.	No exceptions noted.

Control Environment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
	Employee performance is reviewed annually.	Inspected performance appraisal documentation for a sample of employees to determine that performance appraisals were completed during the period.	No exceptions noted.
	A comprehensive Code of Business Conduct and Ethics policy describes employee and contractor responsibilities and expected behavior regarding data and information system usage. The policy is shared with employees and reviewed annually.	Inspected the Code of Business Conduct and Ethics policy available internally via the Company intranet to determine that the policy was in place to describe employee and contractor responsibilities and expected behavior regarding data and information system usage, was shared with employees, and was reviewed according to its regular cadence.	No exceptions noted. The policy was reviewed during its normal cadence in December 2023.
	Employees acknowledge the Code of Business Conduct and Ethics policy upon hire.	Inspected acknowledgements for a sample of new employees to determine that new employees acknowledged that they had read and agreed to the Code of Business Conduct and Ethics policy upon hire.	Exception noted. 2 out of a sample of 12 new employees did not acknowledge the Code of Business Conduct and Ethics policy upon hire.
	The Company has documented disciplinary actions in a formalized sanctions policy for employees and contractors who violate the Code of Business Conduct and Ethics.	Inspected the Code of Business Conduct and Ethics to determine that the Company had documented disciplinary actions in a formalized sanctions policy for employees and contractors who violated the Code of Business Conduct and Ethics.	No exceptions noted.

Control Environment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The hiring manager reviews and approves employee job descriptions.	Inspected system workflows and templates to determine that job descriptions were reviewed and approved by the hiring manager and included authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	No exceptions noted.

Information and Communication			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		
	Internal audits are performed annually, results are communicated to management and the Audit Committee, and corrective actions are monitored.	Inspected internal audit results to determine that an internal audit was performed during the period and corrective actions were monitored and communicated to management and the Audit Committee.	No exceptions noted.
	Vulnerability scanning is performed continuously.	Inspected vulnerability scanning configurations to determine that vulnerability scanning was performed continuously.	No exceptions noted.
	Vulnerabilities identified in the vulnerability scans and penetration testing are remediated in accordance with the threat and vulnerability management policy.	Inspected remediation plans for a sample of vulnerabilities identified in the vulnerability scans and annual penetration test to determine that remediation plans were developed and changes were implemented to remediate all vulnerabilities identified during the continuous scans and penetration test in accordance with the threat and vulnerability management policy.	No exceptions noted.
	A log management tool is utilized to identify trends that may have a potential impact on the Company's ability to achieve its security objectives and generates alerts when specific events occur.	Inspected the log management tool configurations to determine that a log management tool was utilized to identify trends that may have had a potential impact on the Company's ability to achieve its security objectives and generated alerts when specific events occurred.	No exceptions noted.

Information and Communication			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
	Employees are required to complete security awareness training at least annually.	Inspected training completion evidence for a sample of employees to determine that employees were required to complete security awareness training during the period.	Exceptions noted. 2 out of a sample of 44 employees did not complete the required security awareness training during the period.
	During on-boarding, new employees are delivered security awareness training to introduce them to where to find resources and minimum standards and where to ask questions.	Inspected training completion evidence for a sample of new employees to determine that new employees were delivered security awareness training during onboarding to introduce them to where to find resources and minimum standards and where to ask questions.	No exceptions noted.
	Management has established defined roles and responsibilities to oversee the implementation of the security and control environment.	Inspected the Atlassian Security Policy to determine that management had established defined roles and responsibilities to oversee the implementation of the security and control environment.	No exceptions noted.
	The hiring manager reviews and approves employee job descriptions.	Inspected system workflows and templates to determine that job descriptions were reviewed and approved by the hiring manager and included authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	No exceptions noted.
	Significant changes made to key products and services are communicated to internal users and customers.	Inspected internal and external Atlassian sites to determine that significant changes made to key products and services were communicated to internal users and customers.	No exceptions noted.

Information and Communication			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	A whistleblower process is established and accessible to both external individuals and employees.	Inspected the whistleblower hotline documentation to determine that a whistleblower process was established and accessible to both external individuals and employees.	No exceptions noted.
	The Executive Team reviews, sets, and/or revises strategic operational objectives quarterly. The targets are cascaded down into each of the product groups for execution by the Management Team.	Inspected strategy and planning documentation to determine that the Executive Team reviewed, set, and/or revised strategic operational objectives during the period and that they were cascaded down into each of the product groups for execution by the Management Team.	No exceptions noted.
	System boundaries, product descriptions, and key services are documented in detail on both the Atlassian intranet and the customer-facing website.	Inspected customer-facing websites and Atlassian intranet to determine that system boundaries, product descriptions, and key services were documented in detail on both the Atlassian intranet and the customer-facing website.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.		
	The terms of service (ToS) and Data Processing Addendum (DPA) communicate Atlassian's commitments and the customer responsibilities. The ToS and DPA are published on the Atlassian customer-facing website, and any changes are communicated.	Inspected the Atlassian ToS and DPA to determine that the Company's commitments and the customer responsibilities were communicated to customers via the customer-facing website and that changes were communicated.	No exceptions noted.
	Vendor agreements, including any security, availability, and confidentiality commitments, are reviewed during the procurement process for all critical vendors.	Inspected contracts for a sample of critical vendors to determine that vendor agreements, including any security, availability, and confidentiality commitments, were reviewed during the procurement process for all critical vendors.	No exceptions noted.

Information and Communication			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Significant changes made to key products and services are communicated to internal users and customers.	Inspected internal and external Atlassian sites to determine that significant changes made to key products and services were communicated to internal users and customers.	No exceptions noted.
	Users may report bugs; defects; or security, availability, and confidentiality issues.	Inspected the customer reporting portal to determine that users were able to report bugs; defects; or security, availability, and confidentiality issues.	No exceptions noted.
	System availability is published to provide assistance to users for the handling and reporting of incidents.	Inspected the Atlassian status page to determine that system availability was published to provide assistance to users for the handling and reporting of incidents.	No exceptions noted.
	Atlassian communicates changes to confidentiality and security commitments.	Inspected the Atlassian website to determine that changes to confidentiality and security commitments were communicated.	No exceptions noted.

Risk Assessment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.		
	The design of controls and mitigation strategies are reviewed annually.	Inspected the Atlassian Risk and Compliance review documentation to determine that the design of controls and mitigation strategies were reviewed during the period.	No exceptions noted.
	A risk management policy is made available to employees and reviewed annually.	Inspected the risk management policy to determine that the policy was made available to employees and reviewed during the period.	No exceptions noted.
	Atlassian has defined an Enterprise Risk Management (ERM) process and conducts an enterprise risk assessment annually, which includes key product stakeholders.	Inspected the ERM Program to determine that an ERM process was defined and an enterprise risk assessment was performed during the period that included key product stakeholders.	No exceptions noted.
		Inspected the ERM Program to determine that a defined risk assessment process was in place and that risks were documented with a risk rating and assigned a risk owner.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.		
	A risk management policy is made available to employees and reviewed annually.	Inspected the risk management policy to determine that the policy was made available to employees and reviewed during the period.	No exceptions noted.
	Atlassian has defined an Enterprise Risk Management (ERM) process and conducts an enterprise risk assessment annually, which includes key product stakeholders.	Inspected the ERM Program to determine that an ERM process was defined and an enterprise risk assessment was performed during the period that included key product stakeholders.	No exceptions noted.

Risk Assessment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected the ERM Program documentation to determine that a defined risk assessment process was in place and that risks were documented with a risk rating and assigned a risk owner.	No exceptions noted.
	A fraud risk assessment is performed annually by the Director of Risk and Compliance or delegate. A cross-functional survey of employees in areas susceptible to fraud is conducted and combined with an evaluation of external risks. The report results are evaluated and included within the enterprise risk assessment, which is communicated to the board and executive-level managers annually.	Inspected the fraud risk assessment to determine that a fraud risk assessment was performed during its normal cadence by the Director of Risk and Compliance or delegate, that a cross-functional survey of employees in areas susceptible to fraud was conducted and combined with an evaluation of external risks, and that report results were evaluated and included within the enterprise risk assessment that was communicated to the board and executive-level managers during its normal cadence.	No exceptions noted. The fraud risk assessment occurred during its normal cadence in November 2023.
	A disaster recovery policy is shared on the Company intranet and reviewed annually.	Inspected the disaster recovery policy and Company intranet to determine that the disaster recovery policy was reviewed during the period and shared on the Company intranet.	No exceptions noted.
	A disaster recovery plan is in place and tested quarterly.	Inspected the disaster recovery plan and tests to determine that a disaster recovery plan was in place and tested during the period.	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.		
	A risk management policy is made available to employees and reviewed annually.	Inspected the risk management policy to determine that the policy was made available to employees and reviewed during the period.	No exceptions noted.

Risk Assessment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Atlassian has defined an Enterprise Risk Management (ERM) process and conducts an enterprise risk assessment annually, which includes key product stakeholders.	Inspected the ERM Program to determine that an ERM process was defined and an enterprise risk assessment was performed during the period that included key product stakeholders.	No exceptions noted.
		Inspected the ERM Program to determine that a defined risk assessment process was in place and that risks were documented with a risk rating and assigned a risk owner.	No exceptions noted.
	A fraud risk assessment is performed annually by the Director of Risk and Compliance or delegate. A cross-functional survey of employees in areas susceptible to fraud is conducted and combined with an evaluation of external risks. The report results are evaluated and included within the enterprise risk assessment, which is communicated to the board and executive-level managers annually.	Inspected the fraud risk assessment to determine that a fraud risk assessment was performed during its normal cadence by the Director of Risk and Compliance or delegate, that a cross-functional survey of employees in areas susceptible to fraud was conducted and combined with an evaluation of external risks, and that report results were evaluated and included within the enterprise risk assessment that was communicated to the board and executive-level managers during its normal cadence.	No exceptions noted. The fraud risk assessment occurred during its normal cadence in November 2023.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.		
	A risk management policy is made available to employees and reviewed annually.	Inspected the risk management policy to determine that the policy was made available to employees and reviewed during the period.	No exceptions noted.
	Atlassian has defined an Enterprise Risk Management (ERM) process and conducts an enterprise risk assessment annually, which includes key product stakeholders.	Inspected the ERM Program to determine that an ERM process was defined and an enterprise risk assessment was performed during the period that included key product stakeholders.	No exceptions noted.

Risk Assessment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected the ERM Program documentation to determine that a defined risk assessment process was in place and that risks were documented with a risk rating and assigned a risk owner.	No exceptions noted.
	A fraud risk assessment is performed annually by the Director of Risk and Compliance or delegate. A cross-functional survey of employees in areas susceptible to fraud is conducted and combined with an evaluation of external risks. The report results are evaluated and included within the enterprise risk assessment, which is communicated to the board and executive-level managers annually.	Inspected the fraud risk assessment to determine that a fraud risk assessment was performed during its normal cadence by the Director of Risk and Compliance or delegate, that a cross-functional survey of employees in areas susceptible to fraud was conducted and combined with an evaluation of external risks, and that report results were evaluated and included within the enterprise risk assessment that was communicated to the board and executive-level managers during its normal cadence.	No exceptions noted. The fraud risk assessment occurred during its normal cadence in November 2023.
	Penetration testing is performed at least annually.	Inspected penetration test results to determine that penetration testing was performed during the period.	No exceptions noted. The penetration test occurred during its normal cadence in October 2023.
	Vulnerabilities identified in the vulnerability scans and penetration testing are remediated in accordance with the threat and vulnerability management policy.	Inspected remediation plans for a sample of vulnerabilities identified in the vulnerability scans and annual penetration test to determine that remediation plans were developed and changes were implemented to remediate all vulnerabilities identified during the continuous scans and penetration test in accordance with the threat and vulnerability management policy.	No exceptions noted.

Monitoring Activities			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.		
	Internal audits are performed annually, results are communicated to management and the Audit Committee, and corrective actions are monitored.	Inspected internal audit results to determine that an internal audit was performed during the period and corrective actions were monitored and communicated to management and the Audit Committee.	No exceptions noted.
	Penetration testing is performed at least annually.	Inspected penetration test results to determine that penetration testing was performed during the period.	No exceptions noted. The penetration test occurred during its normal cadence in October 2023.
	Vulnerability scanning is performed continuously.	Inspected vulnerability scanning configurations to determine that vulnerability scanning was performed continuously.	No exceptions noted.
	Vulnerabilities identified in the vulnerability scans and penetration testing are remediated in accordance with the threat and vulnerability management policy.	Inspected remediation plans for a sample of vulnerabilities identified in the vulnerability scans and annual penetration test to determine that remediation plans were developed and changes were implemented to remediate all vulnerabilities identified during the continuous scans and penetration test in accordance with the threat and vulnerability management policy.	No exceptions noted.
	SOC 2 reports of critical vendors are reviewed annually.	Inspected SOC 2 report review documentation for a sample of critical vendors to determine that SOC 2 reports of critical vendors were reviewed during the period.	No exceptions noted.

Monitoring Activities			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Suppliers who host or process data undergo an assessment to ensure security, availability, and confidentiality requirements are met.	Inspected attestation review documentation for the subservice organization to determine that the supplier who hosted or processed data underwent an assessment during its normal cadence to ensure security, availability, and confidentiality requirements were met.	No exceptions noted. The supplier assessment occurred during its normal cadence in April 2024.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.		
	Internal audits are performed annually, results are communicated to management and the Audit Committee, and corrective actions are monitored.	Inspected internal audit results to determine that an internal audit was performed during the period and corrective actions were monitored and communicated to management and the Audit Committee.	No exceptions noted.
	SOC 2 reports of critical vendors are reviewed annually.	Inspected SOC 2 report review documentation for a sample of critical vendors to determine that SOC 2 reports of critical vendors were reviewed during the period.	No exceptions noted.
	Suppliers who host or process data undergo an assessment to ensure security, availability, and confidentiality requirements are met.	Inspected attestation review documentation for the subservice organization to determine that the supplier who hosted or processed data underwent an assessment during its normal cadence to ensure security, availability, and confidentiality requirements were met.	No exceptions noted. The supplier assessment occurred during its normal cadence in April 2024.

Control Activities			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.		
	The design of controls and mitigation strategies are reviewed annually.	Inspected the Atlassian Risk and Compliance review documentation to determine that the design of controls and mitigation strategies were reviewed during the period.	No exceptions noted.
	Atlassian has defined an Enterprise Risk Management (ERM) process and conducts an enterprise risk assessment annually, which includes key product stakeholders.	Inspected the ERM Program to determine that an ERM process was defined and an enterprise risk assessment was performed during the period that included key product stakeholders.	No exceptions noted.
		Inspected the ERM Program documentation to determine that a defined risk assessment process was in place and that risks were documented with a risk rating and assigned a risk owner.	No exceptions noted.
	A risk management policy is made available to employees and reviewed annually.	Inspected the risk management policy to determine that the policy was made available to employees and reviewed during the period.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.		
	The design of controls and mitigation strategies are reviewed annually.	Inspected the Atlassian Risk and Compliance review documentation to determine that the design of controls and mitigation strategies were reviewed during the period.	No exceptions noted.

Control Activities			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Atlassian has defined an Enterprise Risk Management (ERM) process and conducts an enterprise risk assessment annually, which includes key product stakeholders.	Inspected the ERM Program to determine that an ERM process was defined and an enterprise risk assessment was performed during the period that included key product stakeholders.	No exceptions noted.
		Inspected the ERM Program documentation to determine that a defined risk assessment process was in place and that risks were documented with a risk rating and assigned a risk owner.	No exceptions noted.
	A risk management policy is made available to employees and reviewed annually.	Inspected the risk management policy to determine that the policy was made available to employees and reviewed during the period.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.		
	Formal procedures are documented that outline the process the Company's staff follows to perform the following system access control functions: - Adding new users - Modifying an existing user's access - Removing an existing user's access - Restricting access based on separation of duties and least privilege	Inspected system access control procedures to determine that formal procedures were documented that outlined the process the Company's staff followed to perform the following system access control functions: - Adding new users - Modifying an existing user's access - Removing an existing user's access - Restricting access based on separation of duties and least privilege	No exceptions noted.
	A security policy is shared and reviewed annually.	Inspected the Atlassian Security Policy to determine that a security policy was shared and reviewed during the period.	No exceptions noted.

Control Activities			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Policies are posted and available online and reviewed at least annually.	Inspected the Company intranet to determine that policies were posted and available online and reviewed during the period.	No exceptions noted.
	A risk management policy is made available to employees and reviewed annually.	Inspected the risk management policy to determine that the policy was made available to employees and reviewed during the period.	No exceptions noted.
	Formal procedures are documented that outline the process the Company's staff follows to back up and recover customer data.	Inspected backup and recovery procedures to determine that formal procedures were documented that outlined the process the Company's staff followed to back up and recover customer data.	No exceptions noted.
	A data classification policy is in place to support the safety and security of data Atlassian holds.	Inspected the data classification policy to determine that a data classification policy was in place to support the safety and security of data Atlassian holds.	No exceptions noted.
	Formal procedures are documented that outline requirements for vulnerability management and system monitoring. The procedures are reviewed at least annually.	Inspected formal vulnerability management and system monitoring procedures to determine that they were documented, were reviewed during the period, and outlined the requirements for vulnerability management and system monitoring.	No exceptions noted.
	A vendor management program is in place. Components of this program include: - Maintaining a list of critical vendors - Requirements for critical vendors to maintain their own security practices and procedures - Annually reviewing attestation reports for critical vendors or performing a vendor risk assessment	Inspected the vendor management policy to determine that a vendor management program was in place and components of this program included: - Maintaining a list of critical vendors - Requirements for critical vendors to maintain their own security practices and procedures - Annually reviewing attestation reports for critical vendors or performing a vendor risk assessment	No exceptions noted.

Control Activities			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	A formal systems development life cycle (SDLC) methodology is in place that governs the development, acquisition, implementation, changes, and maintenance of information systems and related technology requirements.	Inspected SDLC documentation to determine that a formal SDLC methodology was in place that governed the development, acquisition, implementation, changes, and maintenance of information systems and related technology requirements.	No exceptions noted.
	Formal data retention and disposal procedures are documented to guide the secure retention and disposal of Company and customer data.	Inspected data retention and disposal procedures to determine these procedures for secure retention and disposal of Company and customer data were formally documented.	No exceptions noted.
	An incident management policy is shared on the Company intranet and reviewed annually.	Inspected the incident management policy and Company intranet to determine that an incident management policy was reviewed during the period and shared on the Company intranet.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.		
	Two-factor authentication is required when launching an application from the SSO system (Idaptive and Okta).	Inspected system configurations and observed a remote login session to determine that two-factor authentication was required when launching an application from the SSO system (Idaptive and Okta).	No exceptions noted.
	Active Directory (AD) enforces password settings in line with the Atlassian Password Standard. Single Sign On (SSO) allows users to have a single point of authentication to access multiple applications. Password settings for SSO are enforced by AD via the AD connector. The Atlassian Password Standard includes an 8-character minimum, 6 passwords remembered, and lockout after 5 invalid attempts for all passwords (unless there is a system limitation).	Inspected AD password configurations and the Atlassian Password Standard to determine that AD enforced password settings in line with the Atlassian Password Standard, which included an 8-character minimum, 6 passwords remembered, and lockout after 5 invalid attempts for all passwords (unless there is a system limitation).	No exceptions noted.
		Inspected the system configurations to determine that SSO allowed users to have a single point of authentication to access multiple applications and that password settings for were enforced by AD via the AD connector.	No exceptions noted.
	A formal inventory of production system assets that includes asset owners is maintained, and changes to the inventory are logged.	Inspected the production system asset inventory to determine that a formal inventory of production system assets that included asset owners was maintained and changes to the inventory were logged.	No exceptions noted.
	Customer data is logically isolated through the use of unique identifiers.	Inspected system configurations to determine that customer data was logically isolated through the use of unique identifiers.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Cryptographic mechanisms are implemented or enabled to prevent unauthorized disclosure and modification of data at rest.	Inspected encryption configurations for in-scope systems to determine that cryptographic mechanisms were implemented or enabled to prevent unauthorized disclosure and modification of data at rest.	No exceptions noted.
CC6.2	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 requires a valid customer support request or the existence of an active incident that requires access to be resolved.	Inspected support requests for a sample of customer data access requests to determine that access to customer data required a valid customer support request or the existence of an active incident that required access to be resolved.	No exceptions noted.
	The provisioning of service and product accounts is based on job role and function and requires manager approval prior to access being provisioned.	Inspected access logs for a sample of logical access requests to determine that the provisioning of service and product accounts was based on job role and function and required manager approval prior to access being provisioned.	No exceptions noted.
	Okta accounts and network access are automatically disabled within three business days from the time an employee is marked as terminated in the HR system.	Inspected termination tickets and Okta access logs for a sample of terminated employees to determine that a termination ticket was completed and access was revoked within three business days of termination as part of the termination process.	Exception noted. 1 out of a sample of 3 terminated employees did not have their logical access revoked within three business days of termination. An additional sample of 2 terminated employees was selected for testing, and logical access was revoked within

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
			three business days for both employees in the additional sample.
	Active directory accounts and network access are automatically disabled within 8 hours from the time an employee is marked as terminated in the HR system.	Inspected configurations to determine that active directory accounts and network access were automatically disabled within 8 hours from the time an employee was marked as terminated in the HR system.	No exceptions noted.
	Access to internal systems and tools is reviewed at least quarterly, and issues identified are remediated in a timely manner.	Inspected access review documentation to determine that access reviews of internal systems and tools were performed during the period.	No exceptions noted.
	A portion of the control did not operate during the period because the circumstances that warrant the partial operation of the control did not occur during the period. No issues were identified during the quarterly access review performed during the period.	Inquired of management and inspected the quarterly access review to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether issues identified in the access reviews were remediated in a timely manner.	Not tested. No issues were identified as a result of the quarterly access review that occurred during the period.
	Access to products and services is reviewed at least quarterly, and issues identified are remediated in a timely manner.	Inspected user access reviews for products and services to determine that access reviews of products and services were performed during the period.	No exceptions noted.
	A portion of the control did not operate during the period because the circumstances that warrant the partial operation of the control did not occur during the period. No issues were identified during the quarterly access review performed during the period.	Inquired of management and inspected the quarterly access review to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether issues identified in the access reviews were remediated in a timely manner.	Not tested. No issues were identified as a result of the quarterly access review that occurred during the period.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC6.3	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 of duties, to meet the entity's objectives.		
	Access to customer data requires a valid customer support request or the existence of an active incident that requires access to be resolved.	Inspected support requests for a sample of customer data access requests to determine that access to customer data required a valid customer support request or the existence of an active incident that required access to be resolved.	No exceptions noted.
	Privileged access to internal systems and tools, including access to migrate to production, is restricted based on job description.	Inspected access listings, inquired of management, and compared each user's level of access to their job role to determine that privileged access to internal systems and tools, including access to migrate to production, was restricted based on job description.	No exceptions noted.
	Privileged access products and services, including access to migrate to production, is restricted based on job description.	Inspected access listings, inquired of management, and compared each user's level of access to their job role to determine that privileged access to products and services, including access to migrate to production, was restricted based on job description.	No exceptions noted.
	The provisioning of service and product accounts is based on job role and function and requires manager approval prior to access being provisioned.	Inspected access logs for a sample of logical access requests to determine that the provisioning of service and product accounts was based on job role and function and required manager approval prior to access being provisioned.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Access to internal systems and tools is reviewed at least quarterly, and issues identified are remediated in a timely manner.	Inspected access review documentation to determine that access reviews of internal systems and tools were performed during the period.	No exceptions noted.
	A portion of the control did not operate during the period because the circumstances that warrant the partial operation of the control did not occur during the period. No issues were identified during the quarterly access review performed during the period.	Inquired of management and inspected the quarterly access review to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether issues identified in the access reviews were remediated in a timely manner.	Not tested. No issues were identified as a result of the quarterly access review that occurred during the period.
	Multi-factor authentication is used for privileged accounts unless there is a system limitation.	Inspected system configurations and observed login attempts to determine that multi-factor authentication was used for privileged accounts unless there was a system limitation.	No exceptions noted.
	Active directory accounts and network access are automatically disabled within 8 hours from the time an employee is marked as terminated in the HR system.	Inspected configurations to determine that active directory accounts and network access were automatically disabled within 8 hours from the time an employee was marked as terminated in the HR system.	No exceptions noted.
	Okta accounts and network access are automatically disabled within three business days from the time an employee is marked as terminated in the HR system.	Inspected termination tickets and Okta access logs for a sample of terminated employees to determine that a termination ticket was completed and access was revoked within three business days of termination as part of the termination process.	Exception noted. 1 out of a sample of 3 terminated employees did not have their logical access revoked within three business days of termination. An additional sample of 2 terminated employees was selected

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
			for testing, and logical access was revoked within three business days for both employees in the additional sample.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup 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 centers, which are carved out for the purposes of this report.	Not applicable.	Not applicable.
CC6.5	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.		
	A formal inventory of production system assets that includes asset owners is maintained, and changes to the inventory are logged.	Inspected the production system asset inventory to determine that a formal inventory of production system assets that included asset owners was maintained and changes to the inventory were logged.	No exceptions noted.
	Storage media containing sensitive data and licensed software is removed and securely overwritten prior to disposal.	Inspected certificates of destruction for a sample of purged or destroyed media to determine that storage media containing sensitive data and licensed software was removed and securely overwritten prior to disposal.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
	Multi-factor authentication is used for privileged accounts unless there is a system limitation.	Inspected system configurations and observed login attempts to determine that multi-factor authentication was used for privileged accounts unless there was a system limitation.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Two-factor authentication is required when launching an application from the SSO system (Idaptive and Okta).	Inspected system configurations and observed a remote login session to determine that two-factor authentication was required when launching an application from the SSO system (Idaptive and Okta).	No exceptions noted.
	External interfaces to the products and services and key internal interfaces are managed and monitored to prevent unauthorized use or access.	Inspected firewall and/or security group rules to determine that external interfaces to the products and services and key internal interfaces were managed and monitored to prevent unauthorized use or access.	No exceptions noted.
	Infrastructure supporting the service is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected patching evidence and a sample of vulnerability remediation to determine that infrastructure supporting the service was patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service were hardened against security threats.	No exceptions noted.
	IT asset management software is used to enforce hard drive encryption, user authentication requirements, and security patching on Mac/Windows endpoints.	Inspected IT asset management software configurations to determine that tooling was configured to enforce hard drive encryption, user authentication requirements, usage restrictions, authorizations, and security patching for Mac/Windows endpoints.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC6.7	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 meet the entity's objectives.		
	IT asset management software is used to enforce hard drive encryption, user authentication requirements, and security patching on Mac/Windows endpoints.	Inspected IT asset management software configurations to determine that tooling was configured to enforce hard drive encryption, user authentication requirements, usage restrictions, authorizations, and security patching for Mac/Windows endpoints.	No exceptions noted.
	Cryptographic mechanisms are implemented to prevent unauthorized disclosure and modification of data in transit.	Inspected transmission protocol configurations to determine that cryptographic mechanisms were implemented to prevent unauthorized disclosure and modification of data in transit.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.		
	Malicious code protection is implemented on endpoints and servers.	Inspected anti-malware configurations to determine that malicious code protection was implemented on endpoints and servers.	No exceptions noted.
	External interfaces to the products and services and key internal interfaces are managed and monitored to prevent unauthorized use or access.	Inspected firewall and/or security group rules to determine that external interfaces to the products and services and key internal interfaces were managed and monitored to prevent unauthorized use or access.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC7.1	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.		
	Vulnerability scanning is performed continuously.	Inspected vulnerability scanning configurations to determine that vulnerability scanning was performed continuously.	No exceptions noted.
	Vulnerabilities identified in the vulnerability scans and penetration testing are remediated in accordance with the threat and vulnerability management policy.	Inspected remediation plans for a sample of vulnerabilities identified in the vulnerability scans and annual penetration test to determine that remediation plans were developed and changes were implemented to remediate all vulnerabilities identified during the continuous scans and penetration test in accordance with the threat and vulnerability management policy.	No exceptions noted.
	Atlassian has defined an Enterprise Risk Management (ERM) process and conducts an enterprise risk assessment annually, which includes key product stakeholders.	Inspected the ERM Program to determine that an ERM process was defined and an enterprise risk assessment was performed during the period that included key product stakeholders.	No exceptions noted.
		Inspected the ERM Program documentation to determine that a defined risk assessment process was in place and that risks were documented with a risk rating and assigned a risk owner.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC7.2	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 analyzed to determine whether they represent security events.		
	A log management tool is utilized to identify trends that may have a potential impact on the Company's ability to achieve its security objectives and generates alerts when specific events occur.	Inspected the log management tool configurations to determine that a log management tool was utilized to identify trends that may have had a potential impact on the Company's ability to achieve its security objectives and generated alerts when specific events occurred.	No exceptions noted.
	Vulnerability scanning is performed continuously.	Inspected vulnerability scanning configurations to determine that vulnerability scanning was performed continuously.	No exceptions noted.
	Vulnerabilities identified in the vulnerability scans and penetration testing are remediated in accordance with the threat and vulnerability management policy.	Inspected remediation plans for a sample of vulnerabilities identified in the vulnerability scans and annual penetration test to determine that remediation plans were developed and changes were implemented to remediate all vulnerabilities identified during the continuous scans and penetration test in accordance with the threat and vulnerability management policy.	No exceptions noted.
	Penetration testing is performed at least annually.	Inspected penetration test results to determine that penetration testing was performed during the period.	No exceptions noted. The penetration test occurred during its normal cadence in October 2023.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The availability and capacity of each service and its underlying infrastructure are monitored continuously through the use of monitoring tools. Alerts are automatically sent to on-call engineers when early warning thresholds are crossed on key operational metrics.	Inspected the availability and capacity monitoring tools and alert configurations to determine that the availability and capacity of each service and its underlying infrastructure were monitored continuously through the use of monitoring tools and alerts were automatically sent to on-call engineers when early warning thresholds were crossed on key operational metrics.	No exceptions noted.
CC7.3	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.		
	Security events are reviewed and handled in accordance with Incident Management procedures and plans to support the Atlassian mission and business processes and systems, which includes the evaluation, logging, tracking, and communication of all events.	Inspected a sample of security events to determine that security events and incidents were reviewed and handled in accordance with Incident Management procedures and plans to support the Atlassian mission and business processes and systems, which included the evaluation, logging, tracking, and communication of all events.	No exceptions noted.
	Penetration testing is performed at least annually.	Inspected penetration test results to determine that penetration testing was performed during the period.	No exceptions noted. The penetration test occurred during its normal cadence in October 2023.
	Vulnerability scanning is performed continuously.	Inspected vulnerability scanning configurations to determine that vulnerability scanning was performed continuously.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Vulnerabilities identified in the vulnerability scans and penetration testing are remediated in accordance with the threat and vulnerability management policy.	Inspected remediation plans for a sample of vulnerabilities identified in the vulnerability scans and annual penetration test to determine that remediation plans were developed and changes were implemented to remediate all vulnerabilities identified during the continuous scans and penetration test in accordance with the threat and vulnerability management policy.	No exceptions noted.
	An incident management policy is shared on the Company intranet and reviewed annually.	Inspected the incident management policy and Company intranet to determine that an incident management policy was reviewed during the period and shared on the Company intranet.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.		
	Security incidents are reviewed and handled in accordance with Incident Management procedures and plans to support the Atlassian mission and business processes and systems which includes the evaluation, logging, tracking, and communication of all incidents. The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No security incidents occurred during the period.	Inquired of management and inspected security event documentation to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether all security incidents were reviewed and handled in accordance with Incident Management procedures and plans to support Atlassian mission and business processes and systems which included the evaluation, logging, tracking, and communication of all incidents.	Not tested. No security incidents were identified during the period.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	An incident management policy is shared on the Company intranet and reviewed annually.	Inspected the incident management policy and Company intranet to determine that an incident management policy was reviewed during the period and shared on the Company intranet.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.		
	A disaster recovery policy is shared on the Company intranet and reviewed annually.	Inspected the disaster recovery policy and Company intranet to determine that the disaster recovery policy was reviewed during the period and shared on the Company intranet.	No exceptions noted.
	A disaster recovery plan is in place and tested quarterly.	Inspected the disaster recovery plan and tests to determine that a disaster recovery plan was in place and tested during the period.	No exceptions noted.
	An incident management policy is shared on the Company intranet and reviewed annually.	Inspected the incident management policy and Company intranet to determine that an incident management policy was reviewed during the period and shared on the Company intranet.	No exceptions noted.
	Security incidents are reviewed and handled in accordance with Incident Management procedures and plans to support the Atlassian mission and business processes and systems which includes the evaluation, logging, tracking, and communication of all incidents. The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No security incidents occurred during the period.	Inquired of management and inspected security event documentation to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether all security incidents were reviewed and handled in accordance with Incident Management procedures and plans to support Atlassian mission and business processes and systems which included the evaluation, logging, tracking, and communication of all incidents.	Not tested. No security incidents were identified during the period.

Change Management			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.		
	Configuration-controlled changes to infrastructure are tested, reviewed, approved, and documented.	Inspected system configurations enforcing requirements to configuration-control changes to infrastructure to determine that configuration-controlled changes to infrastructure were tested, reviewed, approved, and documented.	No exceptions noted.
	Configuration-controlled changes to products and services are tested, reviewed, and approved. Change management responsibilities are segregated among designated personnel.	Inspected system configurations enforcing requirements to configuration-control changes to products and services to determine that configuration-controlled changes to products and services were tested, reviewed, and approved and that change management responsibilities were segregated among designated personnel.	No exceptions noted.
	Emergency changes are approved within three business days after the change has been implemented. The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No emergency changes were implemented during the period.	Inquired of management and inspected the change population to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether emergency changes were approved within three business days of the change implementation.	Not tested. No emergency changes were identified during the period.
	Access to bypass the normal configuration-controlled change process is restricted to authorized personnel only.	Inspected access listings, inquired of management, and compared each user's level of access to their job role to determine that access to migrate emergency changes to production was restricted to authorized personnel only.	No exceptions noted.

Change Management			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Alerts are automatically generated if a change to the enforcement of peer review/pull requests occurs.	Inspected alert configurations to determine an alert is automatically generated when a change to the enforcement of peer review/pull requests occurs.	No exceptions noted.
	Privileged access to internal systems and tools, including access to migrate to production, is restricted based on job description.	Inspected access listings, inquired of management, and compared each user's level of access to their job role to determine that privileged access to internal systems and tools, including access to migrate to production, was restricted based on job description.	No exceptions noted.
	Privileged access products and services, including access to migrate to production, is restricted based on job description.	Inspected access listings, inquired of management, and compared each user's level of access to their job role to determine that privileged access to products and services, including access to migrate to production, was restricted based on job description.	No exceptions noted.

Risk Mitigation			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.		
	A risk management policy is made available to employees and reviewed annually.	Inspected the risk management policy to determine that the policy was made available to employees and reviewed during the period.	No exceptions noted.
	A disaster recovery policy is shared on the Company intranet and reviewed annually.	Inspected the disaster recovery policy and Company intranet to determine that the disaster recovery policy was reviewed during the period and shared on the Company intranet.	No exceptions noted.
	A disaster recovery plan is in place and tested quarterly.	Inspected the disaster recovery plan and tests to determine that a disaster recovery plan was in place and tested during the period.	No exceptions noted.
	An incident management policy is shared on the Company intranet and reviewed annually.	Inspected the incident management policy and Company intranet to determine that an incident management policy was reviewed during the period and shared on the Company intranet.	No exceptions noted.
	A multi-location strategy is employed for production environments to permit the resumption of operations at other availability zones in the event of the loss of a facility.	Inspected availability zone configurations to determine that a multi-location strategy was employed for production environments to permit the resumption of operations at other availability zones in the event of the loss of a facility.	No exceptions noted.
	Databases are replicated to secondary availability zones in real time. Alerts are configured to notify administrators if replication fails.	Inspected replication configurations to determine that databases were replicated to secondary availability zones in real time and that alerts were configured to notify administrators if replication failed.	No exceptions noted.

Risk Mitigation			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC9.2	The entity assesses and manages risks associated with vendors and business partners.		
	SOC 2 reports of critical vendors are reviewed annually.	Inspected SOC 2 report review documentation for a sample of critical vendors to determine that SOC 2 reports of critical vendors were reviewed during the period.	No exceptions noted.
	Suppliers who host or process data undergo an assessment to ensure security, availability, and confidentiality requirements are met.	Inspected attestation review documentation for the subservice organization to determine that the supplier who hosted or processed data underwent an assessment during its normal cadence to ensure security, availability, and confidentiality requirements were met.	No exceptions noted. The supplier assessment occurred during its normal cadence in April 2024.
	Vendor agreements, including any security, availability, and confidentiality commitments, are reviewed during the procurement process for all critical vendors.	Inspected contracts for a sample of critical vendors to determine that vendor agreements, including any security, availability, and confidentiality commitments, were reviewed during the procurement process for all critical vendors.	No exceptions noted.

Additional Criteria for Availability

Availability			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
A1.1	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.		
	System availability is published to provide assistance to users for the handling and reporting of incidents.	Inspected the Atlassian status page to determine that system availability was published to provide assistance to users for the handling and reporting of incidents.	No exceptions noted.
	The availability and capacity of each service and its underlying infrastructure are monitored continuously through the use of monitoring tools. Alerts are automatically sent to on-call engineers when early warning thresholds are crossed on key operational metrics.	Inspected the availability and capacity monitoring tools and alert configurations to determine that the availability and capacity of each service and its underlying infrastructure were monitored continuously through the use of monitoring tools and alerts were automatically sent to on-call engineers when early warning thresholds were crossed on key operational metrics.	No exceptions noted.
A1.2	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.		
	A disaster recovery policy is shared on the Company intranet and reviewed annually.	Inspected the disaster recovery policy and Company intranet to determine that the disaster recovery policy was reviewed during the period and shared on the Company intranet.	No exceptions noted.
	A disaster recovery plan is in place and tested quarterly.	Inspected the disaster recovery plan and tests to determine that a disaster recovery plan was in place and tested during the period.	No exceptions noted.

Availability			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	System data of products and services is backed up at least daily. Restoration testing occurs annually to ensure that data security and integrity is maintained.	Inspected backup configurations and restoration testing documentation to determine that system data of products and services was backed up at least daily and that restoration testing was performed during the period to ensure that data security and integrity was maintained.	No exceptions noted.
	A multi-location strategy is employed for production environments to permit the resumption of operations at other availability zones in the event of the loss of a facility.	Inspected availability zone configurations to determine that a multi-location strategy was employed for production environments to permit the resumption of operations at other availability zones in the event of the loss of a facility.	No exceptions noted.
	Databases are replicated to secondary availability zones in real time. Alerts are configured to notify administrators if replication fails.	Inspected replication configurations to determine that databases were replicated to secondary availability zones in real time and that alerts were configured to notify administrators if replication failed.	No exceptions noted.
	Formal procedures are documented that outline the process the Company's staff follows to back up and recover customer data.	Inspected backup and recovery procedures to determine that formal procedures were documented that outlined the process the Company's staff followed to back up and recover customer data.	No exceptions noted.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.		
	A disaster recovery policy is shared on the Company intranet and reviewed annually.	Inspected the disaster recovery policy and Company intranet to determine that the disaster recovery policy was reviewed during the period and shared on the Company intranet.	No exceptions noted.

Availability			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	A disaster recovery plan is in place and tested quarterly.	Inspected the disaster recovery plan and tests to determine that a disaster recovery plan was in place and tested during the period.	No exceptions noted.
	Formal procedures are documented that outline the process the Company's staff follows to back up and recover customer data.	Inspected backup and recovery procedures to determine that formal procedures were documented that outlined the process the Company's staff followed to back up and recover customer data.	No exceptions noted.
	System data of products and services is backed up at least daily. Restoration testing occurs annually to ensure that data security and integrity is maintained.	Inspected backup configurations and restoration testing documentation to determine that system data of products and services was backed up at least daily and that restoration testing was performed during the period to ensure that data security and integrity was maintained.	No exceptions noted.

Additional Criteria for Confidentiality

Confidentiality			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.		
	A data classification policy is in place to support the safety and security of data Atlassian holds.	Inspected the data classification policy to determine that a data classification policy was in place to support the safety and security of data Atlassian holds.	No exceptions noted.
	Production data is not used in non-production environments as part of the Software Development Lifecycle Procedures.	Inspected the Software Development Lifecycle Procedures to determine that production data was prohibited by the Procedures from being used in non-production environments.	No exceptions noted.
		Observed the test environment to determine that only test data was used in non-production systems or environments.	No exceptions noted.
	Vendor agreements, including any security, availability, and confidentiality commitments, are reviewed during the procurement process for all critical vendors.	Inspected contracts for a sample of critical vendors to determine that vendor agreements, including any security, availability, and confidentiality commitments, were reviewed during the procurement process for all critical vendors.	No exceptions noted.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.		
	Customer data is disposed of, destroyed, or erased automatically upon customer request in accordance with the retention period, or upon termination of services. Any failures in the automatic deletion process are tracked, and customer data is deleted as requested.	Inspected data deletion configurations to determine that customer data was disposed of, destroyed, or erased automatically upon customer request or upon termination of the services.	No exceptions noted.
		Inspected a sample of customer data deletion request failures to determine that data deletion request failures were tracked, and customer data was deleted as requested.	No exceptions noted.

Confidentiality			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Storage media containing sensitive data and licensed software is removed and securely overwritten prior to disposal.	Inspected certificates of destruction for a sample of purged or destroyed media to determine that storage media containing sensitive data and licensed software was removed and securely overwritten prior to disposal.	No exceptions noted.

Section 5

Other Information Provided by Atlassian Corporation Plc That Is Not Covered by the Service Auditor's Report

Management's Response to Testing Exceptions

Service Organization's Controls	Results of Tests	Management's Response
Employees acknowledge the Code of Business Conduct and Ethics policy upon hire.	Exception noted. 2 out of a sample of 12 new employees did not acknowledge the Code of Business Conduct and Ethics policy upon hire.	Management has followed up with the employees who had not signed the Code of Business Conduct and Ethics policy upon hire and confirmed that they have since acknowledged the policy. Atlassian HR has established a process for escalation procedures to Legal for incomplete acknowledgements.
Okta accounts and network access are automatically disabled within three business days from the time an employee is marked as terminated in the HR system.	Exception noted. 1 out of a sample of 3 terminated employees did not have their logical access revoked within three business days of termination. An additional sample of 2 terminated employees was selected for testing, and logical access was revoked within three business days for both employees in the additional sample.	Management confirmed that the identified employee did not access their account post termination date. Management has since implemented automated deprovisioning of logical access to the production environment.
Employees are required to complete security awareness training at least annually.	Exceptions noted. 2 out of a sample of 44 employees did not complete the required security awareness training during the period.	Management confirmed the employees have since completed security awareness training. Management implemented email alerts for past due training and is exploring preventive measures to ensure timely completion of training.