Atlassian PTY Ltd.

Service Organization Controls (SOC) 2 Type 1 Report

Trello Description of System Relevant to Security, Availability, and Confidentiality

As of October 31, 2018

With Independent Service Auditor’s Report
including Description of Criteria and Controls

Table of Contents

Atlassian's Trello

SECTION I: ATLASSIAN'S MANAGEMENT ASSERTION FOR TRELLO

ATLASSIAN

Atlassian PTY Ltd’s Management Assertion

We have prepared the accompanying Trello Description of System Relevant to Security, Availability, and Confidentiality (Description) of Atlassian PTY Ltd. (Service Organization) in accordance with the criteria for a description of a service organization’s system set forth in the Description Criteria DC section 200, *2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2 Report* (Description Criteria). The Description is intended to provide report users with information about the Trello System (System) that may be useful when assessing the risks from interactions with the System as of October 31, 2018 particularly information about system controls that the Service Organization has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria for security, availability, and confidentiality set forth in TSP section 100, *2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

Atlassian uses Amazon Web Services (“AWS” or “subservice organization”) to provide colocation physical access and environmental protection, Google Cloud Storage (“GCS” or “subservice organization”) to retain backup data, Akamai (“subservice organization”) as a content delivery network, and SparkPost (“subservice organization”) for sending email delivery notifications. The Description includes only the controls of Atlassian and excludes controls of the subservice organization. The Description also indicates that certain trust services criteria specified therein can be met only if AWS, GCS, Akamai, and SparkPost’s controls assumed in the design of Atlassian’s controls are suitably designed and operating effectively along with the related controls at the Service Organization. The Description does not extend to controls of AWS, GCS, Akamai, and SparkPost.

The Description also indicates that certain trust services criteria specified in the Description can be met only if complementary user entity controls assumed in the design of Atlassian’s controls are suitably designed and operating effectively, along with related controls at the Service Organization. The Description does not extend to controls of user entities.

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

a. The Description presents the System that was designed and implemented as of October 31, 2018, in accordance with the Description Criteria.

b. The controls stated in the Description were suitably designed and implemented to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated as described and if user entities applied the complementary user entity controls and the subservice organizations applied the controls assumed in the design of Atlassian’s controls as of October 31, 2018.

DocuSigned by:

D9F75B69402F4F6...

Tom Kennedy
Chief Legal Officer

Section II: Independent Service Auditor's Report

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

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

Independent Service Auditor's Report

To the Management of Atlassian PTY Ltd.

Scope

We have examined Atlassian's accompanying Trello Description of System Relevant to Security, Availability, and Confidentiality of its Trello system used as a visual collaboration tool as of October 31, 2018 (Description) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (Description Criteria) and the suitability of the design of controls included in the Description as of October 31, 2018 to provide reasonable assurance that Atlassian's service commitments and system requirements would be achieved based on the trust services criteria for security, availability, and confidentiality set forth in TSP section 100, *2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

Atlassian uses Amazon Web Services ("AWS" or "subservice organization") to provide colocation physical access and environmental protection, Google Cloud Storage ("GCS" or "subservice organization") to retain backup data, Akamai ("subservice organization") as a content delivery network, and SparkPost ("subservice organization") for sending email delivery notifications. 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 system; its controls relevant to the applicable trust services criteria; and the types of complementary subservice organization controls that the service organization assumes have been suitably designed and implemented at AWS, GCS, Akamai, and SparkPost. Our examination did not extend to the services provided by AWS, GCS, Akamai, and SparkPost, and we have not evaluated whether the controls management assumes have been implemented at AWS, GCS, Akamai, and SparkPost have been implemented or whether such controls were suitably designed and operating effectively as of October 31, 2018.

The Description also indicates that Atlassian's controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of Atlassian's controls are suitably designed and implemented, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

The information in the accompanying Section V: Other Information Provided by Atlassian is presented by management of Atlassian to provide additional information and is not part of Atlassian's Description. Such information has not been subjected to the procedures applied in our examination and, accordingly we express no opinion on it.

Atlassian'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 the service commitments and system requirements were achieved. Atlassian has provided the accompanying assertion titled, Atlassian Pty Ltd.'s Management Assertion for Trello (Assertion) about the presentation of the Description based on the Description Criteria and suitability of the design of the controls described therein to provide reasonable assurance that the service commitments and system requirement would achieved based on the applicable trust services criteria. Atlassian is responsible for (1) preparing the Description and Assertion; (2) the completeness, accuracy, and method of presentation of the Description and Assertion; (3) providing the services covered by the Description; (4) identifying the risks that would threaten the achievement of the service organization's service commitments and system requirements; and (5) designing, implementing, and documenting controls that are suitably designed to meet the applicable trust services criteria stated in the Description.

Service auditor's responsibilities

Our responsibility is to express an opinion on the presentation of the Description and on the suitability of the design of the controls described therein to meet the applicable trust services criteria, based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the Description is presented in accordance with the Description Criteria, and (2) the controls described therein are suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved if operating effectively based on the applicable trust services criteria as of October 31, 2018. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- obtaining an understanding of the system and the service organization's service commitments and system requirements

- performing procedures to obtain evidence about whether the description is presented in accordance with the Description Criteria.
- performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization would achieve its service commitments and system requirements based on the applicable trust services criteria if the controls operated effectively.
- assessing the risks that the Description is not presented in accordance with the Description Criteria and that the controls were not suitably designed to meet 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 users and may not, therefore, include every aspect of the system that each individual user may consider important to its own particular needs.

Because of their nature, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the presentation of the Description, or conclusions about the suitability of the design of the controls to meet the applicable trust services criteria is subject to the risk that the system may change or that controls at a service organization may become ineffective.

Other matter

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

Opinion

In our opinion, in all material respects:

a. the Description presents the Trello system that was designed and implemented as of October 31, 2018 in accordance with the Description Criteria.

b. the controls stated in the Description were suitably designed as of October 31, 2018, to provide reasonable assurance that Atlassian’s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date.

Building a better
working world

Restricted use

This report is intended solely for the information and use of Atlassian, user entities of Atlassian's Trello system as of October 31, 2018 and prospective user entities, independent auditors and practitioners providing services to such user entities, 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, subservice organizations, or other parties, including complementary user entity controls and subservice organization controls assumed in the design of the service organization's controls
- Internal control and its limitations
- User entity responsibilities and how they interact with related controls at the service organization
- The applicable trust services criteria
- The risks that may threaten the achievement of the applicable trust services criteria 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.

Ernst + Young LLP

San Jose, California
December 28, 2018

Section III: Trello Description of System Relevant to Security, Availability, and Confidentiality

Trello Description of System
Relevant to Security, Availability, and Confidentiality

Scope and Purpose of the Report

This report describes the control structure of Atlassian PTY Ltd. (hereinafter "Atlassian" or "company") as it relates to Atlassian's Trello system used as a visual collaboration tool (hereinafter "the System") as of October 31, 2018 for the Security, Availability, and Confidentiality Trust Services Principles.

The description is intended to provide Trello customers, prospective customers, and auditors with information about the system controls related to the criteria for the Security, Availability, and Confidentiality Trust Services Principles set forth in the Description Criteria DC section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* ("Description Criteria") and the suitability of the design of the controls included in the Description as of October 31, 2018 to provide reasonable assurance that Atlassian's service commitments and system requirements would be achieved based on the trust services criteria for security, availability, and confidentiality set forth in TSP section 100, *2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (applicable trust criteria)*. This description may not provide information about Atlassian's Trello system controls that do not relate to the Applicable Trust Services Criteria.

Company Overview and Background

Atlassian was founded in 2002 by Scott Farquhar and Mike Cannon-Brookes. Atlassian had its Initial Public Offering ("IPO") in 2015. Atlassian has offices in San Francisco and Mountain View, California, Sydney, Australia, Manila, Philippines, Yokohama, Japan, Amsterdam, Netherlands, Austin, Texas, and Bengaluru, India.

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

The system in-scope for this report is primarily the Trello system hosted at Amazon Web Services ("AWS") and the supporting IT infrastructure and business processes. This report does not include add-ons, marketplace applications, plugins, and billing services.

Overview of Products and Service

Trello is a visual collaboration tool that creates a shared perspective on any project. Trello helps teams to get a shared perspective on projects through a system of boards, lists, and cards. Trello lets teams organize and prioritize personal lives and work in a fun, flexible, and rewarding way. Trello is available to teams via web or dedicated apps across desktop and mobile platforms.

Infrastructure

Trello is hosted at Amazon Web Services ("AWS") data centers, using the AWS Infrastructure as a Service offering ("IaaS"). The services that make up the Trello system are primarily isolated within a single large private network, which is spread out across up to 5 failure domains (or Availability Zones) for redundancy and fault-tolerance.

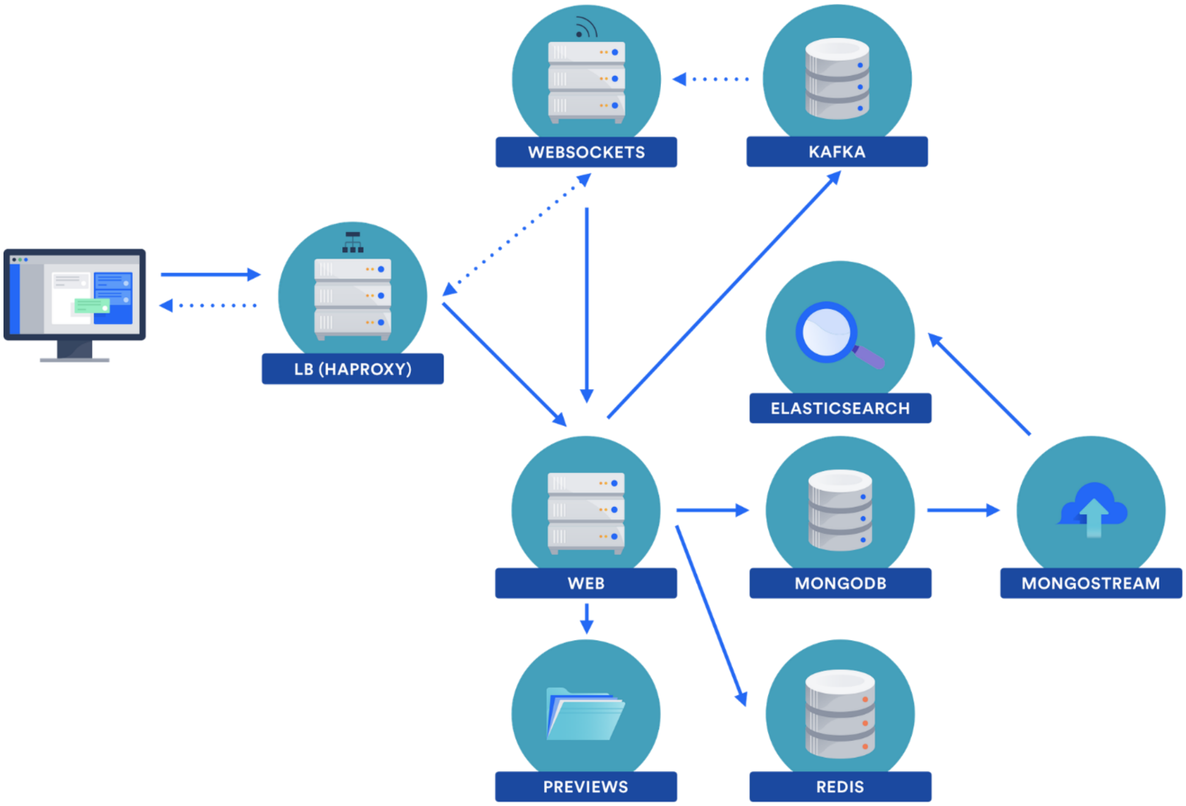

Figure 1: Trello's Infrastructure

The core application is composed of the following 5 services within Atlassian's network:

- **Data Storage:** MongoDB, which is hosted on services in AWS, is used to store customer data within Trello.
- **Messaging Queue and Delivery:** Kafka, RabbitMQ, and SQS are messaging queue solutions used within Trello to facilitate real-time updates. Updates are propagated to appropriate users via the Web Socket Service.
- **Load Balancers and Network Connections:** HAProxy is used as the load balancer to ensure that incoming traffic is properly sorted by type and evenly distributed amongst application nodes. Akamai is used to terminate customers' HTTPS connections, as well as connect customers to the API and web socket services via local POPs.
- **Indexing of Data:** AWS ElasticSearch is used for indexing data for the purposes of Search.

- **Data Caching:** Redis is used for data caching and lookups

The load balancers and Redis are out of scope for this report. Only the messaging queue services, access to the database, and backups of customer data are in scope for this report.

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

Servers

AWS provides Infrastructure as a Service ("IaaS") and the initial creation of the virtual servers, which run Trello. However, the software and operating system configurations are managed by Atlassian's Trello team using a configuration management system (Puppet).

Database

Trello's primary datastore is a MongoDB cluster within the private network, which is hosted in AWS and managed by the Trello Systems Team. The MongoDB cluster is sharded and its nodes are spread out of a minimum of 3 Availability Zones for fault-tolerance and redundancy.

Search indexes are stored within an ElasticSearch cluster, which is also managed by the Trello team, and also hosted within the private network on AWS.

User attachments are stored within Amazon S3 to increase durability guarantees, and segregate attachments using a unique identifier that is stored in the Trello database. The unique identifier that ties the file objects to the user, as well as the board or card the attachment was uploaded to.

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

Software

The following software, services, and tools support the Trello control environment and are in scope as part of the controls and processes being executed:

- Akamai – Global edge; DDoS mitigation and reverse proxy
- AWS ElasticSearch – Indexing of data
- AWS Glacier - Data archiving and long-term backup storage service
- AWS S3 - Stores attachments for Trello
- Bamboo – Bamboo is Atlassian's developed continuous integration tool used to perform automated testing and deployment activities
- Bitbucket Cloud – Atlassian's developed source code and development projects tool
- Centrify – Single sign on service used for Atlassian
- GoogleAuth - Single sign on service used for Atlassian
- Google Cloud Storage ("GCS") – Redundant offsite backup storage location
- HelpScout – Customer support tool
- Impraise – performance feedback tool

- Jira - Ticketing system used for incident management, user access provisioning, and change management process.
- Kafka – Message queue service
- Lever – Hiring tool
- Nagios – System monitoring and alerting platform
- PagerDuty – Alerting tool for monitoring of availability
- Puppet - open-source software configuration management tool
- RabbitMQ - Message queue service
- SparkPost – Outgoing email service provider
- Splunk – Monitoring of security and availability tool
- SQS - Message queue service managed by AWS
- Trello – Used for development, backlog planning, execution, and team coordination
- Workday – Human Resource (HR) system

AWS, GCS, Akamai, and SparkPost are managed by third-party vendors. Atlassian performs a review of the SOC 2 reports for these vendors. The evaluation of the SOC 2 report is performed and reviewed by the Risk and Compliance Team, which includes an assessment of complimentary user entity controls, subservice organizations, and mapping of the controls to key risks. If there are exceptions, Atlassian will review the severity and impact of the exceptions, and if needed, follow up with the individual vendor. Centrify, GoogleAuth, Impraise, Lever, Nagios, PagerDuty, HelpScout, Kaka, Splunk, SQS, RabbitMQ, and Workday are managed by third-party vendors; however, customer data is not stored in these applications. These are supporting and monitoring tools, and are only applicable to support certain controls and criteria.

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

Data

Customers can sign up for Trello using the www.trello.com website or via Trello's mobile apps. Upon accepting the terms and conditions, and completing the sign-up flow, a new database record and unique identifier are created in MongoDB for that customer account. The unique ID is used thereafter for associating data with the specific user account. The data is logically separated from other users' data using these unique ID's. All user created data are similarly assigned unique identifiers such that they can be correctly associated to users, teams, enterprises, and so on.

Customers whose accounts are provisioned from an external enterprise single sign-on solution follows the same process as non-SSO accounts except for the one-time import of the customers' personal detail from the external identify provider. Customers are responsible for the security and confidentiality of the data prior to the import.

All production customer data is encrypted in transit and also encrypted at rest within Atlassian's network, which is managed by AWS. AWS' SOC 2 report is reviewed at least annually by Atlassian. Customer attachments in Trello are encrypted in the AWS S3 platform. Additionally, there is no production data residing in the non-production environments.

Organizational Structure

Atlassian's organizational structure is managed by a committee consisting of Human Resources, Financial Planning and Analysis, as well as Senior Management and Leadership (including the Co-Founders).

The following organizational chart identifies the teams responsible for human resources, strategic planning, education/training, legal matters, business growth/modeling, finance, accounting, and technology operations:

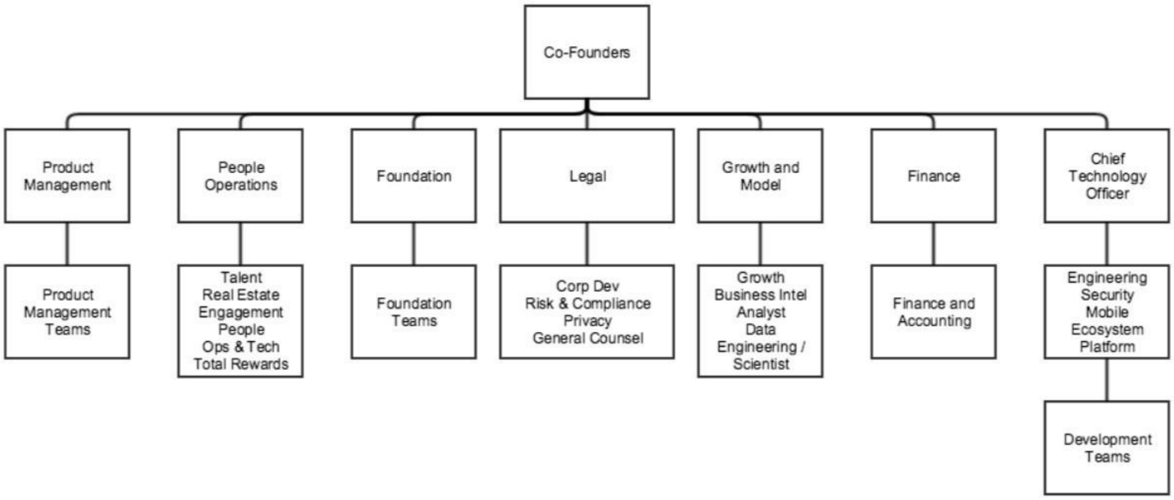
Co-Founders
Product Management
People Operations
Foundation
Legal
Growth and Model
Finance
Chief Technology Officer
Product Management Teams
Talent Real Estate Engagement People Ops & Tech Total Rewards
Foundation Teams
Corp Dev Risk & Compliance Privacy General Counsel
Growth Business Intel Analyst Data Engineering / Scientist
Finance and Accounting
Engineering Security Mobile Ecosystem Platform
Development Teams

Figure 2: Atlassian's Organizational Chart

The organizational charts are reviewed by appropriate Atlassian management and updated semi-annually. Additionally, organizational charts are automatically updated based on employee action notices and is available to all Atlassian employees via Atlassian's HR system, Workday.

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

- Product Management - focuses on validating the demands of customers, provides insight and guidance around minimum viable product and user experience.
- People Operations (in partnership with the people leaders) - focuses on determining the right talent strategy to deliver against the needs of Atlassian. People team is responsible for talent acquisition and learning, total rewards and technology, and workplace experiences.

- Foundation - Exists to harness the resources of Atlassian to champion organizations who believe that education is the key to eliminate disadvantage. This is accomplished by improving educational outcomes in developing countries, increasing skill-based volunteering and leveraging Atlassian's products.
- Legal - responsible for matters related to corporate development, privacy, general counsel operations, public relations, risk and compliance.
- Growth and Model - responsible for monitoring business trends, analytics, data engineering and data science.
- Finance - responsible for handling finance and accounting
- Chief Technology Officer (Technology Operations) - oversees Engineering, Security, Mobile, Ecosystem and Platform.
    - Head of Engineering, Software Teams oversees all operations for the products.
    - Development Manager:
        - Drives and improves product quality and innovation, team productivity, manages simultaneous projects in an agile fashion, customer satisfaction and product supportability.
        - Coordinate multiple streams of software development, involving multiple teams, geographic distribution and indirect reports
        - Collaborate with Product Management by contributing to roadmaps, setting priorities, and providing estimates
        - Collaborate with Customer Support to help ensure customer success and drive quality improvements
        - Promote, define, refine and enforce best practices and process improvements that fit Atlassian's agile methodology
        - Provide visibility through metrics and project status reporting
        - Set objectives for people and teams and holds them accountable
        - Work with Recruitment to attract and hire outstanding individuals to create high performing balanced teams
        - Lead by example and practice an inclusive management style.

Policies and Procedures

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

1. Are properly communicated throughout the organization
2. Are properly owned, managed and supported
3. Clearly outline business objectives
4. Show commitment to meet regulatory obligations
5. Are focused on continual iteration and improvement
6. Provide for an exception process
7. Support the Policy Framework and Structure

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

Item	Defines	Explanation
Policy	General rules and requirements ("state")	Outlines specific requirements or rules that must be met.
Standard	Specific details ("what")	Collection of system-specific or procedural-specific requirements that must be met by everyone.
Guideline	Common practice, recommendations and suggestions	Collection of system specific or procedural specific "suggestions" for best practice. 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 guidelines, it is a set of instructions on how to accomplish a task. From a compliance perspective, a procedure is also referred to as "Control Activity". The goal of a process/procedure is to help ensure 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 they are relevant and appropriately manage risk in accordance with Atlassian's risk appetite. Changes are reviewed by the Atlassian Policy Committee ("APC"), and approved by the corresponding Policy Owner.

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

Policy Review Process

In order to advance a policy, standard, guideline, or standard operating procedures to be publicly available internally to all Atlassian employees, each document should go through a review process. The review process follows Atlassian's internal process where feedback is sought from a small group of knowledgeable peers on the topic. After feedback is incorporated, the draft document is submitted to the Policy Committee, either via email or via the internal corporate chat system. Any announcements of changes or updates to policies, standards or guidelines can be shared via the Blog on Policy Central.

Relevant Aspects of the Control Environment, Risk Assessment, Control Activity, Monitoring, and Information and Communication

Control Environment

The objectives of Atlassian's control environment are to set the tone for the organization's internal control.

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

Atlassian's Board of Directors and various subcommittees (including Nominating and Governance, Compensation and Leadership Development) meet at least annually to review committee charters and corporate governance, which defines their roles, responsibilities, member qualifications, meeting frequency, and other discussion topics. Meeting minutes of the annual meetings are recorded, which include participants and date the meeting occurred.

The executive team sets strategic operational objects at least annually during Values, Targets, Focus and Metrics (VTFM) sessions. Each target is communicated down into each of the product groups for execution by the Management Team. Progress toward targets is evaluated at least quarterly by the Executive and Management Teams.

The audit committee charter is published on Atlassian's Investor's website under Governance Documents. Within the audit committee charter, it includes the roles, responsibilities, key activities, and meetings. Qualifications for the audit committee's "Financial Officer" are also outlined and defined within the audit committee charter. Audit Committee meeting calendar and meeting agenda are developed. The audit committee meeting is published annually as well. Results of the audit committee meeting results are published after the meeting has completed. The agenda includes items to be discussed, and also includes general questions and answers about the annual general meeting such as who is allowed to vote at the annual general meeting.

Management Controls and Operating Style

The control environment at Atlassian entails the involvement and ongoing engagement of Executive and Senior Management. The Risk and Compliance team engages the Executive and Senior Management in various ways:

1. Standards - Atlassian follows specific standards that enables the organization to exercise practices around security, availability, quality, reliability and confidentiality.
2. Tools - Atlassian leverages tools designed specifically to assist in identifying, analyzing, tracking, deciding, implementing and monitoring risks and findings. In addition, the tools allow the company to effectively communicate and collaborate using workflows to help ensure activities are properly tracked. The use of customized tools allows them to be more closely integrated with the standard way of how Atlassian operates: specific, scalable, systematic and robust.
3. Enterprise Risk Management Process - Atlassian uses an Enterprise Risk Management process that is modeled after ISO 31000:2009 "Risk Management - Principles and Guidelines".

4. Unified approach - As Atlassian becomes involved across various best practice, legal and regulatory requirements, it becomes more essential to create control activities that are universal and not unique to specific standards and guidelines. Instead of tracking control activities specific to a standard, Atlassian tracks activities that are universal and meet multiple standards. This approach has enabled Atlassian to speak a common language across the organization. Along with a unified approach comes operational efficiency and a way to more effectively establish a controlled environment.

Integrity, Ethical Values, and Competence

The integrity, ethical values and competence are key elements of Atlassian's control environment. Atlassian employees are required to acknowledge the Code of Conduct, Insider Trading Policy, FCPA and Anti-Corruption Policy. The HR Operations team is involved in helping ensure these policies and agreements are acknowledged and background screening is followed through. Employees and contractors with access to Atlassian systems are asked to re-acknowledge on an annual basis.

The Atlassian Code of Conduct covers the following:

- Standards of Conduct
- Compliance Procedures

All Atlassian employees are assigned a task in the Workday HR system to acknowledge the Code of Conduct, Insider Trading Policy, and FCPA and Anti-Corruption Policy. The Human Resources Operations team reviews Workday for completion of the task and follows up with employees when the task is not completed.

Atlassian has a documented Code of Conduct policy and process to help ensure that all employees complete the acknowledgement. An operational control is provided by the Workday system generated task assignment, which allows a report to capture any employees that have not completed acknowledgement of Atlassian's Code of Conduct. A process for follow up in these cases is documented.

Learning and Development

Atlassian requires anti-harassment training and also offers opportunities for technical training and professional development. In regards to technical training and professional development, every Atlassian employee has the ability to reach their fullest potential and do the best work of their lives by providing the right support. Autonomy, mastery and purpose are cornerstones of this philosophy. Therefore, Atlassian lowers the barriers of entry for new learning, making it possible for employees to take charge of their learning needs and own more of one's growth and development. Atlassian offers professional development for employees via training or tuition reimbursements and online learning management systems.

AccelerateU is Atlassian's primary learning and development hub to help employees pursue new ways to learn and grow. Everything from custom growth plan templates to online resources and other learning experiences are available through AccelerateU. The learning hub provides growth support for all levels of employees at Atlassian.

- Growth Plans were 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. The Learning and Development team has done extensive research to map formalized competencies to the majority of roles at Atlassian, particularly those that are customer and product facing. Managers and employees use these competencies to see what is required for success in a position and what areas an employee needs further development/training around. Based on these gaps, managers and the Learning and Development team can recommend training, self-study, or coaching as needed.
- Degreed is an extensive third-party tool Atlassian can use to access thousands of online learning resources for free. It also serves as the primary portal to host internally-created learning paths that guide employees through targeted learning experiences, whether they are new hires, new managers, or seasoned employees taking their first steps into people leadership.

Human Resource Policies and Procedures

Atlassian has a job posting process and job advertisement template for all recruiters and team members to determine what needs to be included in each job advertisement. All Atlassian job ads are required to pass an approval process before they are posted on the careers page. The job ad is created by the recruiter and hiring manager. Additionally, a team reviews posted job ads for consistency, spelling/grammar, diversity friendly verbiage, etc.

The recruiting process is based on prior relevant experience, educational background and a clear understanding of integrity and ethical behavior. As part of the hiring process, interview feedback is collected in the applicant tracking system, Lever, for all candidates that participate in an onsite interview. Each interviewer, hiring manager and HR member has access to Lever, and is able to view the candidates' profile. A recruiter will not initiate an offer for hire without receiving a minimum of 1 interview review in Lever prior to their start date. The exception to this process is contractors. For contractors who are hired outside of the standard hiring process and outside of Lever, there is a confirmation screening step in the on-boarding process within the Service Desk.

Roles and responsibilities are documented in job ads as well as within the online applicant tracking system. Background checks are also performed and results are reviewed against a results matrix and escalated to Legal and Head of HR Operations, if needed. Background checks are performed by Atlassian for all full-time new hires. For contractors who are hired as part of an agency, background checks are not performed by Atlassian, but rather, the agency. Atlassian has a contract with all agencies to help ensure that background checks are performed.

Upon hiring, a 90-day on-boarding plan is provided to all new employees as part of the on-boarding process with Atlassian to get them up to speed on their role, responsibilities and become acclimated to the culture. In addition, confidentiality and protection of company assets are clearly communicated and acknowledged by new hires. The HR Operations team delivers the plan to the employee during the on-boarding communications process. Atlassian also requires that all employees and independent contractors sign a Confidential Information and Invention Assignment ("CIIA") Agreement.

A weekly review is performed to determine that new employees have signed the CIIA and that background checks are completed prior to their start date.

Once a year, Atlassian people leaders host performance check-ins with their team members to have a two-way conversation about how each team member contributed to Atlassian's success for the previous 12 months and to identify opportunities for improvement. After the check-in feedback process closes, the managers then provide performance and relative contribution ratings for all those on their team. The final stage of performance appraisals is Atlassian's salary planning process for providing potential merit increases.

Manual presentations, reminders, and trainings are used to communicate the process to Atlassian employees. In addition, system controls provided by Impraise (for check-Ins) and Workday (for relative contribution and salary planning) track that all eligible Atlassian employees participate in performance reviews.

Risk Assessment

An Enterprise Risk Management ("ERM") process is in place to manage risks associated with the company strategy and business objectives.

Atlassian utilizes a process which:

- Establishes the context, both internal and external, as it related to the company business objectives
- Assesses the risks
- Facilitates development of strategies for risk treatment
- Communicates the outcome
- Monitors the execution of the risk strategies, as well as changes to the environment

The Enterprise Risk Management process is modeled after ISO31000-2009 "Risk Management - Principles and Guidelines"

When performing a risk assessment under the ERM framework, risk is considered holistically on its impact to the organization, not just to individual function/department/product that is directly impacted by the risk. While there may be specifics for a particular function, product or service, they are always considered in terms of affecting the entire company. This principle is followed, not only in the analysis but also in evaluation of the risks (e.g. a risk that is critical for product A and low for Atlassian is evaluated as low). Nevertheless, if in the course of the analysis a significant concern is discovered for a particular function, product or service, this is flagged for subsequent follow up.

To perform activities supporting the ERM, various sources of information are crucial to encompass all areas of the organizations. Information sources include but are not limited to:

- Business goals and objectives - High level business goals and objectives, and the strategies in place to achieve these goals and objectives.

- Major initiatives - Large projects and initiatives that could have significant impact on the company's risk profile. Additionally, Risk and Compliance managers are engaged by various teams and they bring their knowledge of the environment into consideration.
- Risk and Compliance assessments - Throughout the period, Atlassian performs a number of periodic and ad-hoc assessments, which includes key product stakeholders. Results of the assessments are captured in the Atlassian Governance, Risk, and Compliance (GRC) tool.
- Incidents - Atlassian utilizes a common Incident Management Process ("IM"), including Post Incident Review ("PIR"). The goal of PIR is not only to establish the root cause but also to create actions aimed at reducing the risk of repeated incident.
- Organizational policies - Organizational policies that have been put in place to achieve the organization's strategic goals and objectives.
- Interviews with major stakeholders and subject matter experts ("SME") - As part of the structured Enterprise Risk Assessment Atlassian interviews all members of the Management team and engage with SME as needed.
- Other sources - Atlassian may consult industry publications, analyses, incidents, etc., as necessary.
- Internal and external context of the ERM process includes but is not limited to understanding:
    - Competitive environment - who are Atlassian's major competitors, what threat level they present, what are the trends in Atlassian's industry
    - Legal/Regulatory environment - what are Atlassian's obligations within their operating jurisdictions, what are the industry standards Atlassian needs to abide by
    - Financial environment - current status as well as trends in the financial and currency markets that could affect us, perceptions and values of external stakeholders
    - Technological environment - what are the trends in technology and software development
    - Business environment - markets that Atlassian is currently in or plans to enter, what is the perception of Atlassian and its products/services, what are the current developments and trends in Atlassian's ecosystem, major vendors and customers
    - Human environment - what are the social and cultural trends that could affect us, what are the current status and trends of the talent pools where Atlassian currently has or plans to establish presence
    - Natural environment - considerations related to natural disasters, and office locations and facilities

The goal of establishing the external context is to identify potential key drivers and trends that could impact the organization.

- Organizational structure, governance, roles and accountabilities
- Short and long-term strategies, objectives, initiatives, programs and projects
- Resources and capabilities (capital, people, skillsets, technologies, facilities)
- Operations (processes, services, systems)
- Organizational culture and values
- Information, information flow and decision making
- Policies and standards
- Vendor agreements and dependencies

The goal of establishing the internal context is to identify potential key internal misalignments between strategy, objectives, capabilities and execution.

The Risk and Compliance function plays a crucial role in Atlassian's ability to integrate ERM through the organization. The risk assessment process entails the following:

- Identification of risks
- Analysis of risks identified
- Evaluation of the risks
- Treatment of the risks

Throughout all stages of the ERM process, the Risk and Compliance team communicates with the relevant stakeholders and consults with appropriate subject matter resources.

All risks and associated treatment plans (e.g. mitigating actions) are recorded in the GRC. Links to detailed treatment plans, along with individual tasks are also established. Risk and Compliance team monitors the progress and provides oversight of the plans execution. Progress review is part of the operational business function meetings, as well as periodic updates to the risk owners and Executive Operations.

The Atlassian Risk and Compliance team monitors the environment of internal control and identifies significant changes that have occurred. The Risk and Compliance team meets on a weekly basis with bi-annual strategic planning to discuss:

- Risk and Compliance strategic direction
- Changes happening within the organization that affect Risk and Compliance efforts and initiatives
- Changes happening outside of Atlassian that affect Risk and Compliance efforts and initiatives
- The Risk and Compliance pipeline of how Atlassian approaches risk and compliance with internal customers
- Changes to existing and ingesting of new compliance standards

Entity Level and Financial Risk

A fraud risk assessment is performed annually by the Head of Risk and Compliance. A cross-functional survey of employees in areas susceptible to fraud is conducted and combined with an evaluation of external risks. The results of the survey are consolidated into a report by an independent third-party company, which identifies and ranks areas of risk within the company. The head of risk and compliance reviews the risks and recommendations, and addresses them on a case-by-case basis. If needed, the recommendations will be added to Atlassian's Entity Risk Management ("ERM") and (Entity Risk Management Assessment ("ERMA"). The results are included with the enterprise risk assessment which is communicated to the board and executive level managers annually.

A whistleblower hotline is established and is accessible to both external individuals and employees within the Company. The whistleblower hotline is included within the Code of Conduct which all employees are required to certify that they received. If an individual calls the Whistleblower hotline the General Counsel, Associate General Counsel and Audit Committee Chair receive a notification with the details of the claim. If a claim is received it is discussed at the next Audit Committee meeting including remediation action and resolution. To ensure that the whistleblower hotline notification system is operating properly it is tested every six months.

Annually, a standard disclosure checklist is completed by a member of Technical Accounting to identify areas for disclosure. The Head of Technical Accounting and Financial Reporting reviews an electronic copy of the checklist for completeness and accuracy of responses provided and evidences review and approval via Jira Service Desk. The Corporate Controller reviews the financials and footnote disclosures prepared by the member of Technical Accounting for reasonableness, internal consistency and confirms prior period balances of the final financial statements. A copy of the reviewed statements is attached to an email to the Chief Financial Officer evidencing completion of review.

The Spend Authority Limits (Signature Authority Matrix) is maintained by Legal which establishes the signature authority for expenditures, contracts, capital acquisitions, and write offs. The Limits are reviewed annually at every Board of Directors meeting.

On an annual basis, the Controller reviews the financial statement risk assessments based on knowledge of the Company and also against the assumptions used in the prior year. The controller also ensures that the total net profit and loss amount is within the financial risk assessments and ties to the fiscal year-end financial statements. Materiality threshold and methodology is also reviewed and compared with other companies to determine appropriateness of materiality.

Internal Audit

The Internal Audit team conducts internal audits around Sarbanes-Oxley 404 (SOX), Service Organization Control (SOC 2), International Organization for Standardization (ISO), and operational audits, and results are communicated, and corrective actions monitored. The Internal Audit team engages with third party qualified auditors to perform compliance audits against standards on an annual basis. The results of the audits are captured as findings in the GRC tool and remediation is tracked in the tool with regular reports to management and the

Audit Committee.

Information and Communication

Atlassian constantly updates the customers on their responsibilities as well as those of Atlassian. Communication includes but is not limited to policies, guidelines, customer privacy, security, product changes as well as product alerts. Atlassian also communicates changes to confidentiality commitments to its customers, vendors and internal users through the Atlassian website, when applicable.

Customer responsibilities are described on the Atlassian customer-facing website. The responsibilities include, but are not limited to the following:

- Acceptable use policy
- Reporting copyright and trademark violations
- Customer Agreement
- Designating customers as authorized users
- Guidelines for law enforcement
- Privacy policy
- Reseller agreement
- Professional services agreement
- Service-specific terms
- Third-party code in Atlassian products
- Training terms and policies
- Trademark

Atlassian communicates its commitment that security is a top priority for its customers and Atlassian internal users through Atlassian's Trust Center. A vulnerability and incident portal is available for customers and Atlassian internal users to report any improvements, issues and/or defects related to security. A Cloud Security Statement, Cloud Security Alliance and adherence to ISO27001 are also communicated to customers through the Trust Center FAQ.

In addition, customers and Atlassian internal users are offered multiple methods for contacting Atlassian. Customers and internal users can contact Atlassian via various methods to report issues on bugs, defects, availability, security and confidentiality:

- https://trello.com/contact
- support@trello.com (email)
- Social media and app store reviews
- https://community.atlassian.com
- htpps://trello.com/trust
- public bug site

Atlassian also communicates security, availability, and confidentiality principles to the internal users through the on-boarding process and policies and procedures available in the internal Confluence pages and Rocket Fuel (New Employee On-Boarding).

A description of the Trello system delineating the boundaries and describing relevant components is documented on the Atlassian intranet and the customer-facing website. Any significant changes made to the systems (new feature releases, integrations with other systems, interface updates) are also communicated to customers via the Atlassian customer-facing website. Blog posts generally include links to documentation and support resources that customers can use to troubleshoot issues and contact Atlassian. Availability of the Trello system, including the status and uptime of Trello, is published in the customer-facing website for all customers.

Formal communication is in place to state Atlassian's obligations to both internal and external customers. Internal communications are directed to Atlassian staff to inform of architectural, operational and support obligations for all relevant products and services. The scope of services includes, but are not limited to:

- Load balancers
- Services
- Application node software components
- Persistent and ephemeral storage
- Internal provisioning, configuration, monitoring and platform maintenance

External obligations and product information to customers are communicated via www.atlassian.com and are covered specifically in the following areas:

- Atlassian documentation
    - Getting started
    - Tutorials
    - Integrations with other systems, add-on
    - Administrative capabilities
    - Product collaboration
    - Knowledge base
- Frequently asked questions
- Customer agreement
- Privacy policy
- Professional services agreement

Information Security

Information and information systems are critical to the operations of Atlassian globally. Atlassian takes all appropriate steps to help ensure that all company information, customer information, and information systems are properly protected from threats such as error, fraud, industrial espionage, privacy violation, legal liability and natural disaster.

Information Security Controls

Information security controls are defined as appropriate and compliance with the controls are reviewed by Atlassian's Risk and Compliance team.

Periodic Review of Risks and Controls

The Atlassian security program seeks to balance risk against the cost of implementing controls. A periodic review of risks and security controls will be carried out to address changing business requirements and priorities. All security policies are assessed and reviewed at least on an annual basis. Evaluation of risks and controls are accomplished in line with a Risk Management Program and Compliance Program.

Information Security Training

Appropriate training enables employees to comply with their responsibilities as it relates to the Information Security Policy. The Security team periodically launches company-wide phishing exercises. Exposure rates are tracked and reported to all Atlassian employees to raise the awareness. The report also includes educational material and best practice to avoid future attacks.

Disciplinary Notice

In the event of a violation of the Information Security Policy, employees are required to notify management upon learning of the violation. Employees who violate the Information Security Policy are subject to disciplinary action, up to and including termination of employment.

Description of Control Activities and Relevant Aspects of Operations

A. Change Management

Change initiation

Changes to the Trello platform and its supporting services are planned in Trello, Confluence, and Jira by the product development teams, which include product management, design, engineering, and quality assurance.

Change Development

Atlassian uses an agile development methodology to manage tasks within the team-based development environments.

Trello and its supporting services each have a master source code repository (or master branch) where developers make changes. The branch holds the master copy of source code for developers to work on. Whenever a change is needed, a developer creates a local branch in Atlassian's Bitbucket (source code repository), downloads the branch to their local drive and begins coding. After the code is updated, the developer creates a pull request to merge the code to the master branch. Pull requests use the "merge checks" feature built into Bitbucket to enforce peer review(s) and approval(s) and automated tests (green build tests) before the code can be merged. Bitbucket will not allow a pull request to be approved by the same user who raises it. This prevents any direct changes to the master branch except through a peer-reviewed and tested pull request. If there are any change to the code contained in the pull request, any previous approvals are not counted, and the pull request must be re-approved before it can be merged.

Peer review green build process (PRGB)

Source Code repositories enforce peer review and green build settings using built-in compliance settings. When pushing to Deployment-Bamboo (the workflow system which automatically tests and deploys the software), a process validates that the following settings are enforced:

- Requires >= 1 approver for code changes
- Un-approves automatically if any new changes are made before the release
- Requires successful testing
- Changes without a pull request are not allowed

If the above requirements are not met, the code is rejected.

In addition, changes cannot be made to Trello code unless they have passed a comprehensive regime of automated tests (that help ensure the functionality and integrity of the application is not compromised by the change).

The Trello development team uses the "merge checks" feature built into Bitbucket to enforce review requirements. This prevents any changes to the production branch (the version of application code that is served to all customers) except through a peer-reviewed and tested pull request; direct commits (changes) to the production branch are not allowed. Before a pull request to production can be merged, it must be approved by at least two authorized developers. The author of the pull request cannot provide one of these approvals. If there are any change to the code contained in the pull request, any previous approvals are not counted, and the pull request must be re-approved before it can be merged.

The changes in the pull request must also pass all automated tests that run in Atlassian's Deployment-Bamboo instance. Administrative access to Deployment bamboo is limited to the members of the Build Engineering team.

Change Deployment

After a pull request is merged into the production branch and the team is ready to deploy the new version, the deployment is executed via Deployment Bamboo. Before a build can be created, Deployment Bamboo performs a check to confirm that the PRGB controls are enabled on the source repository. Upon successful check in Deployment Bamboo, a package file is built and a signature is signed or tagged to the package (artifact). An Atlassian-only "Compliance" setting in Bitbucket prevents any of the above controls from being changed or turned off, either via the web UI or the API. If the "Compliance" control itself is turned off for a repository, Bitbucket logs an event to the Atlassian data warehouse, where it triggers an automated alert in the REPCOM system. Any such alerts are routed to the relevant development manager to confirm that no unauthorized changes were made, and to restore the setting.

The Trello production environment only accepts two types of builds: 1) builds that are signed by Deployment Bamboo or 2) builds that have a signed tag from Deployment Bamboo. The deployment will not be successful if a signature or tag is not present on the built package. Only Deployment Bamboo has access to push builds to the production environment. Therefore, only builds made by Deployment Bamboo that have been peer reviewed and tested can be deployed to production. Upon deployment, all customers will receive the same version of Trello product. Major releases are also notified to customers through the customer-facing website.

Privileged access to Deployment Bamboo is restricted to the members of the Build Engineering team and the Build Engineering Development Team Lead performs a review of privileged user access for deployment-bamboo semi-annually.

Scanning of Production Code

Trello utilizes SourceClear to regularly scan and review the code base to detect vulnerable open source libraries being used. The scanner is integrated into the Trello build plan and are run automatically when changes are made to the code base. The scanner is configured to fail a build if any known vulnerabilities are found. Developers periodically review the reports, assess the vulnerabilities, determine the risk and severity level, and triage the findings based on severity level. Different levels of severity will be addressed and prioritized within the development ticket tracking system. Vulnerabilities are reviewed and actioned, if required.

All vulnerabilities are reviewed and actioned, if required.

Deployment Script Changes

Changes to the Deployment Bamboo scripts follow the change management process outlined above. Any changes made to the repositories affecting operating system, system configurations, and other critical hardware follow a peer review and green build process. Code is peer reviewed and once approved, uses Puppet as a method for deployment to a deployment Bamboo system for green build processing/testing. Bitbucket operating system and database configurations are deployed using the Puppet configuration management tool. Configurations are stored in Bitbucket repositories.

Other changes

Any changes made to the repositories affecting operating system, system configurations and other critical hardware follow a peer review and green build process.

Emergency Changes

Emergency changes follow an expedited process, noting that all controls are still adhered to.

B. Logical Access

Provisioning Customer Production Accounts

When creating an account with any of Atlassian's products, the user is directed to acknowledge the standardized customer agreement. An account cannot be made for any of Atlassian's products without first being directed to acknowledge the customer agreement. Upon creation and if updated, the customer agreement is approved by the Legal department.

The customer agreement is standardized across all Atlassian products. This includes customer's responsibilities for security, availability and confidentiality. There are also agreements between Atlassian and channel partners that defines the responsibility and liability for both partners. For end customers who purchased Atlassian products through a channel partner, customers automatically acknowledged the customer agreement. Additionally, channel partners are responsible for helping to ensure customers are legally bound to Atlassian's terms of service that cover commitments over security and confidentiality. From time to time, based on proposed deal size, Atlassian legal may negotiate a master services agreement with certain Enterprise customers.

After acknowledging the customer agreement, the user's request is accepted, and the new user account is provisioned. Users are all assigned unique identifiers upon creation of customer account, which are subsequently used by the Trello system to logically segregate that user's data from that of other user accounts.

De-provisioning Customer Production Accounts

Upon deletion of a user's account (by the user themselves, or their organization's administrator in the case of enterprise accounts), all data regarding that user account is soft-deleted and flagged for permanent erasure within 30 days. Any data saved within backup files are erased within 90 days as per the backup retention policy (see Backups).

If the customer requests their data deleted via a support ticket, support will validate the scope, timeframe, and legitimacy of the request, and if warranted, will create a ticket for engineering to facilitate the deletion. Engineering has crafted a set of tools to perform the deletion safely and consistently.

Production Environment Access

Customer Access

External customers can register for a Trello account using an email address, password, and desired username. Upon sign up, the customer-side team administrators have the ability to invite and grant access to their Trello team following their own designated authorized approver's permission and access provisioning process. Users can only access Trello boards and cards that they are associated and authorized to.

Users can access Trello via the browser user interface, mobile apps, or using Trello's REST API.

Atlassian Internal Users Access

Access to Trello infrastructure is tightly restricted. All services are hosted within the production AWS account. Atlassian must authenticate through Atlassian's two-factor authentication via Duo and a valid SSH key when accessing the infrastructure (if they are in the relevant restricted AD group). Atlassian users also need to be inside Atlassian's network or connected through VPN and connect using the Jumpbox or AWS Console access.

Atlassian access to the underlying AWS accounts, and the corresponding instances providing Trello's datastore, queues, and supporting tools, are restricted to the members of the Trello Systems team.

Additionally, privileged access to production environments is restricted to authorized and appropriate Atlassian users only.

Password

Customer Access

The password settings for Trello customers are governed through password length. The default password policy for external Trello users requires a minimum of 8 characters with no hard expiry.

It is the customers' responsibility to ensure that their accounts are appropriately configured and setup to their corporate network / password and other authentication mechanisms such as Single Sign-On (SAML) or two-factor authentication.

Atlassian Internal Users Access

Passwords are an important part of Atlassian's efforts to protect its technology systems and information assets by helping ensure that only approved individuals can access these systems and assets. For high-risk systems, other approved authentication methods that provide higher levels of assurance and accountability than passwords are used.

Atlassian provides various secured methods to connect to Atlassian production environment. The primary method for connecting to Atlasian resources uses two-factor authentication via Duo and Centrify.

Duo two-factor authentication is required when logging into VPN (Remote Access Service) from any IP address and Centrify single sign-on allows users to have a single point of authentication to access multiple applications. The only exception is when an IP address is whitelisted within the "exempt IP" settings in Centrify.

For Atlassian employees, a minimum of 12 characters is enforced for passwords in Centrify configured in Atlassian's Active Directory.

User Provisioning, Review and De-provisioning of Atlassian Internal Users

Atlassian Internal User Provisioning

Active Directory contains a subset of groups which are automatically created and maintained based on demographic and employment information in the HR Workday system. These groups are based on division, team, location, employment type, and management status. As well as initially provisioning membership, staff member's assigned groups will be updated to reflect a team/department change or termination.

Access to the Atlassian internal network and internal tools is restricted to authorized users via logical access measures:

- Each Atlassian user account must have an active Active Directory account
- Each Atlassian user account must be a member of the appropriate LDAP group

Access to the AWS production environment and supporting tools, in addition to the Workday group access, is provisioned only after appropriate approval via the access request process.

The access request process directs users to submit a request through a creation of a Trello Card on the Trello Systems Access Request ("TSAR") board and appropriately reviewed and approved. Upon appropriate review and approval, access is provisioned, and the Trello Card is marked as "completed".

Atlassian Internal User De-provisioning

De-provisioning of access via terminations are initiated at the Workday level. Human Resources initiates the termination once notified by management via Workday. The system does not permit termination dates to be backdated. Centrify is configured to pull all the upcoming terminations from Workday via a job and then schedules the user to be terminated accordingly in Active Directory. Once terminated via the above process, users are unable to manually connect to the network, login to the Wi-Fi or access via VPN, including remote access via Duo and acess to Trello's backend systems. Additionally, any access to systems whose privileges are not managed by Active Directory, Centrify, Workday, and Google Authentication, will be revoked manually by an administrator upon notification by management.

Atlassian Internal User Role Changes

Role changes are a common practice and Atlassian has a process in place to make any internal transition an effortless and seamless event. When a user changes roles and moves from the Engineering, Support, or Finance group to one of the other areas (Engineering, Support, or Finance groups), an alert is generated and a notification is sent to the Human Resource Information Systems Manager or Workplace Technology team, who is responsible for performing the access review, and for helping ensure timely modification of system access, commensurate with the new role.

Atlassian Internal User Access Reviews

Atlassian's Engineering Managers or Team Leads perform semi-annual privileged user access reviews on Trello and the associated in-scope supporting tools/services. Any discrepancies identified are escalated to the respective managers and are addressed in a timely manner based on the nature of remediation required.

Privileged access to Workday is limited to appropriate users. The People Central Systems Support Specialist performs a review over Workday admin users on a semi-annual basis.

Access of Atlassian Support Team to User Data

Trello has a dedicated group of customer support personnel who help users troubleshoot issues during the course of using Trello. Those support personnel are able to access user data via impersonation only with the express, revocable permission of said user. Impersonation access is granted by the user via a specific in-app mechanism and is not usable without the user's involvement. Any access of user data by support personnel is linked to a valid support case within Helpscout. The ability to initiate an impersonation request is limited to support personnel. Additional personnel may be granted access after review by the Trello operations team.

Public documentation on how to use the services and their features is available on https://help.trello.com.

Vulnerability Scanning

Management of technical vulnerabilities for Atlassian systems is performed using the following:

- Technical vulnerability management is implemented using the Nexpose vulnerability scanners.
- Publicly identified vulnerabilities in Atlassian products are reported to Atlassian via the Atlassian Bug Bounty.
- Internally identified vulnerabilities in Atlassian products and systems are reported to Atlassian via the Security Service Desk.

Regular reviews of all identified Atlassian critical vulnerabilities are conducted daily when applicable and subject matter experts monitor the vendor mailing list for notification of new versions and vulnerabilities.

Atlassian utilizes two network vulnerability scanners one to scan the internal network, and one to scan the external-facing network. Results are emailed to the relevant system owner for triaging and, if they determine it to be necessary, creating a ticket for resolution.

Penetration Testing

Atlassian products are required to participate in a public bug bounty program.

Submissions are initially triaged by Bugcrowd for validity and reproducibility. Valid submissions are then released into Atlassian's Bug Bounty account and triaged by the Security team and assigned a priority level. Jira tickets are raised in individual team Jira instances and/or Trello boards, tagged with the security label, and tracked to resolution.

Endpoint Protection and Asset Management

Atlassian's Windows and Mac machines utilize Active Directory for authentication. Atlassian uses a standard build as a guide when provisioning or re-provisioning new machines with enabled drive encryption and the use of Cylance product for malware protection. Ongoing workstation asset management, security patch deployment, and drive encryption auditing is done using polices deployed through Active Directory (Windows) and Casper (Mac).

Email Scanning

Proofpoint is used to provide malware protection for incoming email at the perimeter. In addition, on an annual basis, Atlassian performs a company-wide phishing exercise on Atlassian employees to educate staff on the risks associated with malware.

Firewall

Atlassian maintains firewalls at the corporate network edges and around production environments. Firewalls are configured using security policy rules maintained by the Network Engineering team and are also in placed at all Atlassian offices. In order to access the production environments, users must be logged on to the Atlassian network (either via the corporate office network or VPN) and therefore, would be protected by the firewall rules.

Firewall rules are in place to restrict access to the production environment and only users that have access to a designated Active Directory group have access to change the firewall rules.

Encryption

Data is encrypted at rest.

Data in transit, including attachment contents, is encrypted with the TLS cryptographic protocol. External users connect to Trello using encrypted traffic via SSL (TLS) protocol. Certificates are rotated when required.

C. Physical Access

Trello is hosted within both AWS and Google facilities. Atlassian reviews the AWS SOC 2 report on an annual basis for completeness, accuracy, and relevance to Atlassian's business needs. Any question or concern in regard to the hosted facility SOC 2 report are followed-up and tracked to resolution on a timely basis.

D. Capacity Management

Trello performs capacity management on an ongoing, as well as scheduled basis. The infrastructure and systems that make up Trello are continuously monitored for utilization levels and adjusted accordingly. In addition to the constant resizing and reconfiguring of systems based on real-time load, Trello conducts quarterly audits of its infrastructure to ensure that the systems are provisioned with enough headroom to handle surges and spikes of user activity, as well as for load-sharing. An effective capacity planning process needs to happen on a perpetual basis to help ensure the projections are accurate and complete. With capacity planning in place, customer needs will be better met, compute and capacity resources will be better optimized for use and capital expenditure forecasting will be more accurately reported for guidance to investors.

E. Backup and Replication

Backups

A rolling live replica of Trello's primary database is constantly being taken on a 1-hour delay. Additionally, a full backup snapshot of the primary database is taken once every 24 hours where the encrypted snapshot is stored in AWS S3 and weekly in Google Cloud Storage.

All Trello backups are retained on the following schedule and at the following locations:

- AWS EC2 on a dedicated backup server for two days
- AWS S3 for 7 days
- Google Cloud Storage for 30 days
- AWS Glacier for 90 days

Monitoring tools are used to monitor and identify data backup failure in both AWS S3 and Google Cloud Storage, along with email alerts sent to the Trello's support team for investigation and resolution. However, AWS and Google Cloud Storage is responsible for the processing of backup and replication of data.

Only authorized members of the Trello operations team have access to the backup locations to allow them to monitor the performance of the backup processes, and in the very unlikely event that a restore becomes necessary. After 90 days, the encrypted backup files are destroyed.

Backup restores are performed monthly in order to test the validity of the backups. Additionally, a full backup of a single production database replica is scheduled to automatically restore on a monthly basis to ensure that production data can be restored.

Replication

Trello utilizes a highly available cluster of MongoDB servers within AWS to store data. The database is split into many pieces or "shards". These shards are each hosted by a redundant set of servers called a Replica Set to allow for horizontal scalability. Each replica set is spread across a minimum of 3 failure domains (Availability Zones) to allow for maximum resiliency against AWS or underlying networking issues.

Disaster recovery

A disaster recovery policy is in place and is reviewed on an annual basis by the disaster recovery steering committee. Procedures for disaster recovery execution are defined, reviewed, tested, and in place. The policy describes, at a high level, the purpose, objectives, scope, critical dependencies, RTO/RPO and roles/responsibilities. Atlassian follows 'ISO22301 Business Continuity' as a guideline to their disaster recovery program.

Disaster recovery tests are performed on a quarterly basis and are performed in a simulated environment. Tabletop exercises are also performed to help the disaster response teams walk through various scenarios of incidents. After disaster recovery tests are performed, outputs of the tests are captured, analyzed and discussed to determine the scope of the next steps for continuous improvement of the tests. The improvement efforts are captured within engineering tickets and followed through as appropriate.

F. Monitoring

The Trello engineering team continuously monitors a vast array of system metrics from across the infrastructure to help ensure users have an excellent service experience. In addition to metrics, a large volume of log information is captured from the various services that comprise Trello as a product. Metrics, logs, and frequent automated system checks are combined into an overall monitoring solution which is used to send automated alerts when collected data points exceed predefined thresholds. These alerts are used to make the Trello engineering team aware of potential incidents such that they can be remediated before any customer-facing impact is realized.

Trello uses tools to monitor the availability and processing capacity of customer-facing services. Changes to availability of user-facing Trello services are published online so that customers may check the real-time and historical status of Trello at any time.

G. Incident Management

An organizational wide incident management process is in place. The Incident management process must meet the Atlassian Incident Management Standard.

The focus of all incident management is to minimize downtime, service degradation or security risk for customers and internal users. Every action in managing an incident is recorded in an Incident Management System under an incident ticket.

The standard principles of Incident management consists of the following:

- Detection and recording - Atlassian has the appropriate tools in place to properly detect and record all incidents.
- Incident Classification for Resolution and Communication - Incidents are classified according to the level of severity. Incident Managers are a crucial part to exercising judgement on the incident priority.
- Communication Steps Based on Severity - The severity of incident determines the communication steps all Incident Managers take.
- Investigation and Diagnosis - Investigations begin with existing runbooks and other relevant documentation. Many incidents have pre-formulated solutions captured in runbooks.
- Resolution and Recovery - The Incident Management team encourages quick and responsive incident resolution and have the ability to resolve incidents immediately.
- Incident Handover - When incidents are escalated and run longer, incident handovers are coordinated.
- Closure and Post Incident Review - Clients/customers have the opportunity to provide feedback on the resolution of the incident. Support or Customer Advocacy confirm the resolution of all customer-reported incidents with the reporting customer. When the incident is completely resolved, the Incident Manager completes and closes all incident records and tickets. After high severity incidents, the Incident Manager completes a Post Incident Review (PIR) which is to be documented. If the root cause is fully understood from a previous incident then the PIR can link to that previous incident.
- Incident Reporting and Analysis - Data from IT incidents, including both those received and resolved by Support are typically analyzed and reported for trends and indications of unidentified problems requiring definition and resolution.
- Relation to Problem Management - Where possible, all related or similar incidents are examined for a common cause. Where incidents temporarily cannot be associated with any particular root cause (Problem), they are reviewed for any other common incidents.

Atlassian uses four Severity levels:

Severity	Description	Examples
0	Crisis incident with maximum impact	• Major Security Incident • Major Outage with Data Loss
1	Critical incident with very high impact	• Outage affecting all users for over one hour

Severity	Description	Examples
2	Major incident with significant impact	• Trello Search down for an hour
3	Minor incident with low impact	• Notification emails delayed by 30 mins

Factors considered when determining severity:

- Length/Duration of an outage - If the rough time it will take to complete an incident is known, Atlassian uses this to help gauge the severity of an incident. Typically incidents with no known ETA will take higher severity levels.
- Number of customers affected - for Cloud, currently 1 instance is classified as 1 customer. Also, the license size of the instances is considered, some bugs only impact bigger Cloud customers, which raises severity. Other services have an estimate of how many customers use the system.
- Customer / Internal service - Customer services such as support.atlassian.com.
- Is there any data loss - any potential data loss to customers increases severity.
- Security risks/breach - especially security breaches that have been made public, or if customer confidentiality has been compromised, or if Atlassian is in violation of the terms of a contractual agreement. These are usually severity 0 if active compromise has occurred.
- Down or degraded - If degraded - how degraded? e.g. Atlassian product being slow might be a lot more impactful than a slow response from support.atlassian.com.

Customers have the ability to report vulnerabilities and incidents via the Company web site: https://www.atlassian.com/trust/security, contacting the support team, and other methods as described within the "Information and Communication" section above. Reported incidents are triaged by the Security team. If the vulnerability and/or incident are considered to be relevant for immediate action, the Security team will escalate via the development team ticketing system for further discussion and prioritization. All other minor requests will be backlogged for future consideration. In addition to incident reporting, an external-facing page is available to display updates on the status of Trello components, system metrics, and a listing of past incidents: https://www.trellostatus.com.

H. Data Classification and Confidentiality of Information

All Atlassian employees share in the responsibility for helping to ensure that information receives an appropriate level of protection by observing the Information Classification policy:

- Information should be classified in terms of legal requirements, value, and criticality to Atlassian
- Information should be labeled to help ensure appropriate handling
- Manage all removable media with the same handling guidelines as below
- Media being disposed of should be securely deleted
- Media containing company information should be protected against unauthorized access, misuse or corruption during transport

The following guidelines are used to classify data at Atlassian:

Rating	Description	Examples
Restricted	Information customers and staff have trusted to Atlassian's protection, which would be very damaging if released. Trust is the operative word.	• Customer Personally Identifiable Information (PII) • Customer credit cards • US Social Security numbers (customer or staff) • Staff personal, bank, and salary details • Sensitive company accounting data • Decryption keys or passwords protecting information at this level • Any other data Atlassian has a strong legal or moral requirement to protect
Public	Information freely available to the public.	• Any information available to the public • Released source code • Newsletters • Information up on web site
Internal	Information internal to Atlassian which would be embarrassing if released, but not otherwise harmful. The default for most Atlassian-generated information.	• Most extranet pages • Jira issues such as invoices or phone records • Unreleased source code • Information only accessible from the office IP's • Product announcements before the release date
Confidential	Information Atlassian holds which could cause damage to Atlassian or its customers if released. The default for any information customers have given us.	• Customer support issues logged on support site • Business plans and deals (including on extranet) • Information under a NDA • Unresolved security issues in Atlassian's products • Third-party closed-source code • Most passwords • Customer source code or other IP stored in Atlassian's hosted products

Subservice Organizations

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

Criteria	Service Organization	Controls
CC5.1 (Logical access)	Amazon Web Services (AWS) Google Cloud Storage (GCS) Akamai SparkPost	Privileged IT access, including administrator accounts, is approved by appropriate personnel prior to access provisioning. IT access privileges are reviewed on a quarterly basis by appropriate personnel. User access to Amazon systems is revoked within 24 hours of the employee record being terminated (deactivated) in the HR System by Human Resources.
CC5.5 (Physical and Environmental Access)	Amazon Web Services (AWS) Google Cloud Storage (GCS)	Physical access to the data centers is approved by an authorized individual. Physical access is revoked within 24 hours of the employee or vendor record being deactivated. Physical access to the data centers is reviewed on a quarterly basis by appropriate personnel. Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited to 30 days by legal or contractual obligations. Physical access points to server locations are managed by electronic access control devices. Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents. Amazon-owned data centers are protected by fire detection and suppression systems. AWS performs periodic reviews of colocation

Criteria	Service Organization	Controls
		service providers to validate adherence with AWS security and operational standards. Google-owned data centers are protected by fire detection and suppression systems. GCS performs periodic reviews of colocation service providers to validate adherence with GCS security and operational standards.
CC 5.7 (Transmission of Data)	Amazon Web Services (AWS) Google Cloud Storage (GCS)	Data is encrypted in transit in AWS and GCS.
CC7.4 (Restore Operations) CC7.5 (Recovery Procedures) CC9.1 (Mitigating Business Disruptions) A1.1 (Forecasts Capacity) A1.2 (Data Backup) A1.3 (Integrity and Completeness of Backup Data)	Amazon Web Services (AWS) Google Cloud Storage (GCS)	Backups of Trello data are performed, stored, and monitored.

Complementary User Entity Controls

Atlassian designed its controls with the assumption that certain controls will be the responsibility of its customers (or "user entities"). The following is a representative list of controls that are recommended to be in operation at user entities to complement the controls of Atlassian's Trello System. This is not a comprehensive list of all controls that should be employed by Atlassian's user entities.

Change Management:

- Customers are responsible for validating the accuracy and completeness of data contained in their Trello account.

Logical Access:

- Customers are responsible for creating a username and password to access their account.
- Customers are responsible for inviting team members and managing team members' access rights to Trello.
- Customers are responsible for establishing their own usage and access policies to their Trello accounts.
- Customers are responsible for identifying approved points of contacts to coordinate with Atlassian.
- Customers are responsible for the appropriate set-up of the following logical security settings: IP whitelisting, 2FA, SAML, and GoogleAuth setup, if applicable.
- Customers are responsible for configuring their own instance according to their organization's policies and procedures.
- Customers are responsible for requesting and approving Atlassian's customer support access to their account.
- Customers are responsible for performing periodic review of access and configurations for appropriateness.
- Customers are responsible for requesting their account to Trello to be removed.

Incident Management:

- Customers are responsible for alerting Atlassian of incidents (related to Security, Availability, and Confidentiality) when they become aware of them.
- Customers are responsible for monitoring or resolving the incident alerts as part of the use of the application.

Backups:

- Customers are responsible for performing periodic backups of their account.

Anti-virus and Data Protection:

- Customers are responsible for running virus scan on all media attachments and its contents.

- Customers are responsible for the security and confidentiality of the data prior to the import.
- Customers are responsible for configuring privacy and security settings for their Trello boards.
- Customers are responsible for having data classification policies relating to posting of information within their Trello boards.
- Customers are responsible for monitoring the confidentiality of data that is posted on their individual Trello boards.

Vendor Management

- Channel partners are responsible for helping to ensure customers are legally bound to Atlassian's terms of service that cover commitments over security and confidentiality.

Add-ons, Plug-ins, and marketplace products:

- Customers are responsible for managing the actions that an add-on and plug-in will have on their instance.

Section IV: Atlassian's Description of Criteria and Controls

Atlassian's Description of Criteria and Controls

Criteria and Controls

On the pages that follow, the applicable Trust Services Criteria and the controls to meet the criteria have been specified by, and are the responsibility of Atlassian.

Procedures for Assessing Completeness and Accuracy of Information Provided by the Entity (IPE)

For the controls requiring the use of IPE, including Electronic Audit Evidence (EAE) (e.g., controls requiring system-generated populations for sample-based testing), we perform a combination of the following procedures where possible based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used: (1) inspect the source of the IPE, (2) inspect the query, script, or parameters used to generate the IPE, (3) tie data between the IPE and the source, and/or (4) inspect the IPE for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintains its integrity. In addition to the above procedures, for controls requiring management's use of IPE in the execution of the controls (e.g., periodic reviews of user access listings), we inspect management's procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

Common Criteria (CC) to All Security, Availability, and Confidentiality Principles
CC1.0 Common Criteria Related to Control Environment

CC	Criteria	Controls of Atlassian
CC1.1	The entity demonstrates a commitment to integrity and ethical values	Policies are posted and available online, assigned a policy owner, and reviewed at least annually.
		At least annually, the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) review committee charters and corporate governance which define their roles, responsibilities, meeting frequency, participants, and member qualifications.
		The process of identifying and reviewing Board of Director Candidates is defined in Nominating and Governance Committee charter.
		The Executive team sets strategic operational objectives annually.
		Employees and contractors acknowledge the Code of Conduct annually.
		Performance appraisals are performed at least annually.
		Vendor agreements, including any security, availability, and confidentiality commitments, are reviewed during the procurement process.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	At least annually, the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) review committee charters and corporate governance which define their roles, responsibilities, meeting frequency, participants, and member qualifications.
		The process of identifying and reviewing Board of Director Candidates is defined In Nominating and Governance Committee charter.
		Audit Committee Charter defines roles, responsibilities and key activities.
		Audit Committee meeting calendar and general meeting agenda are developed.
		Qualifications for the Audit Committee's "Financial Expert" have been defined in the audit committee charter.

Common Criteria (CC) to All Security, Availability, and Confidentiality Principles
CC1.0 Common Criteria Related to Control Environment

CC	Criteria	Controls of Atlassian
CC1.2 (Cont.)		The Atlassian Risk and Compliance team evaluates the design of controls and mitigation strategies in meeting identified risks and recommends changes in the control environment. Atlassian maintains a risk and controls matrix within their GRC tool.
		The Atlassian Risk and Compliance team monitors the environment of internal control and identifies significant changes that have occurred.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	At least annually, the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) review committee charters and corporate governance which define their roles, responsibilities, meeting frequency, participants, and member qualifications.
		The process of identifying and reviewing Board of Director Candidates is defined In Nominating and Governance Committee charter.
		Vendor agreements, including any security, availability, and confidentiality commitments, are reviewed during the procurement process.
		Atlassian reviews the SOC reports of the third-party vendors on an annual basis.
		Hiring manager reviews and approves the job description prior to posting of job ads.
		Organizational charts are perpetually updated based on employee action notices and available to all Atlassian employees via Workday.
		The organizational charts are reviewed by appropriate Atlassian management and updated semi-annually.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Policies are posted and available online, assigned a policy owner, and reviewed by appropriate Atlassian management at least annually.
		At least annually, the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) review committee charters and corporate governance which

Common Criteria (CC) to All Security, Availability, and Confidentiality Principles

CC1.0 Common Criteria Related to Control Environment

CC	Criteria	Controls of Atlassian
CC1.4 (Cont.)		define their roles, responsibilities, meeting frequency, participants, and member qualifications.
		The process of identifying and reviewing Board of Director Candidates is defined In Nominating and Governance Committee charter.
		Vendor agreements, including any security, availability and confidentiality commitments, are reviewed by appropriate Atlassian management during the procurement process.
		Candidates are reviewed and approved by at least two interviewers prior to hiring.
		Background checks are performed prior to a new hire's start date. Results are reviewed against a results matrix and escalated to Legal and Head of HR Operations, if needed.
		User awareness training for phishing risks are part of the Security Awareness program at Atlassian. Additionally, phishing awareness exercises are performed at least on an annual basis.
		Performance appraisals are performed at least annually.
		Training is provided to employees to support their continued development and growth.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Policies are posted and available online, assigned a policy owner, and reviewed at least annually.
		At least annually, the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) review committee charters and corporate governance which define their roles, responsibilities, meeting frequency, participants, and member qualifications.
		New employees are assigned a 90-day onboarding plan.
		Employees and contractors are required to sign CIIAs as part of the onboarding process.
		Employees and contractors acknowledge the Code of Conduct annually.

Common Criteria (CC) to All Security, Availability, and Confidentiality Principles

CC1.0 Common Criteria Related to Control Environment

CC	Criteria	Controls of Atlassian
CC1.5 (Cont.)		Performance appraisals are performed at least annually.
		Training is provided to employees to support their continued development and growth.

Common Criteria (CC) to All Security, Availability, and Confidentiality Principles
CC2.0 Common Criteria Related to Control Environment

CC	Criteria	Controls of Atlassian
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	At least annually, the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) review committee charters and corporate governance which define their roles, responsibilities, meeting frequency, participants, and member qualifications.
		Audit Committee Charter defines roles, responsibilities and key activities.
		Audit Committee Meeting calendar and general meeting agenda are developed.
		Qualifications for the Audit Committee's "Financial Expert" have been defined in the audit committee charter.
		Financial statement risk assessment is reviewed by Controller at least on an annual basis.
		A fraud risk assessment is performed annually by the Head of Risk and Compliance. A cross-functional survey of employees in areas susceptible to fraud is conducted and combined with an evaluation of external risks. Results are evaluated by the Head of Risk and Compliance and a report. The results are included with the enterprise risk assessment which is communicated to the board and executive level managers annually.
		Internal audits are performed, results are communicated and corrective actions monitored.
		Peer review and passed green build testing is required prior to merging the code to the production branch.
		Bitbucket does not allow change pull request to be approved by the same user who requests it.
		Bamboo will not allow code to be deployed unless it has passed green build testing. A green build (successful build) occurs when all the tests as defined within the Bamboo build plan have successfully completed. A red build occurs if any tests defined within the Bamboo build plan fail.

Common Criteria (CC) to All Security, Availability, and Confidentiality Principles

CC2.0 Common Criteria Related to Control Environment

CC	Criteria	Controls of Atlassian
CC2.1 (Cont.)		Deployment Bamboo performs a check to validate that the SOX setting on Bitbucket are compliant to following: * Requires >1 approver * Unapprove automatically on new changes * Changes without a pull request If the settings are not enforced, the code is rejected.
		Trello will not allow code artifacts to deploy or run on the platform unless they have been peer reviewed and have passed green build testing.
		Operating system, database, Puppet, deployment script, and emergency changes follow the same process as the application changes.
		Privileged access to Deployment Bamboo is restricted to the members of the Build Engineering team.
		The Build Engineering Development Team Lead performs a review of privileged user access for deployment-bamboo semi-annually.
		A JIRA ticket is automatically generated if a change to the enforcement of peer review/pull requests occurs.
CC2.2	The entity internally communicates information, including objectives, and responsibilities for internal control, necessary to support the functioning of internal control.	Employees and contractors are required to sign CIIAs as part of the onboarding process.
		New employees are assigned a 90 day onboarding plan
		Employees and contractors acknowledge the Code of Conduct annually.
		A weekly review is performed to determine that the CIIA (Confidential Information and Inventions Assignment) and background checks are completed for new employees prior to their start date.
		User awareness training for phishing risks are part of the Security Awareness program at Atlassian. Additionally, phishing awareness exercises are performed at least on an annual basis.
		At least annually, the Board of Directors and its various subcommittees (including Audit,

Common Criteria (CC) to All Security, Availability, and Confidentiality Principles
CC2.0 Common Criteria Related to Control Environment

CC	Criteria	Controls of Atlassian
CC2.2 (Cont.)		Nominating and Governance, Compensation and Leadership Development) review committee charters and corporate governance which define their roles, responsibilities, meeting frequency, participants, and member qualifications.
		Atlassian has established a Whistleblower hotline that is accessible to both external individuals and employees within the Company.
		Users may report bugs, defects, or availability, security and confidentiality issues.
		An organizational wide incident management process is in place, with the SRE team responsible for incidents and problems for Atlassian services and platforms. Incident management process must meet the Atlassian Incident Management Standard.
		A description of the system delineating the boundaries and describing relevant components is documented on the Atlassian intranet and the customer-facing website.
		Atlassian communicates its commitment to security as a top priority for its customers via Atlassian Trust Security page.
		Atlassian communicates changes to confidentiality commitments through Atlassian's web site, when applicable.
		Significant changes made to the system are communicated to internal users and customers.
		Monitoring tools are in place to track and notify on the availability of Trello systems and services.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	At least annually, the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) review committee charters and corporate governance which define their roles, responsibilities, meeting frequency, participants, and member qualifications.
		Audit Committee Charter defines roles, responsibilities and key activities.

Common Criteria (CC) to All Security, Availability, and Confidentiality Principles
CC2.0 Common Criteria Related to Control Environment

CC	Criteria	Controls of Atlassian
CC2.3 (Cont.)		Audit Committee Meeting calendar and general meeting agenda are developed.
		Qualifications for the Audit Committee's "Financial Expert" have been defined in the audit committee charter.
		A fraud risk assessment is performed annually by the Head of Risk and Compliance. A cross-functional survey of employees in areas susceptible to fraud is conducted and combined with an evaluation of external risks. Results are evaluated by the Head of Risk and Compliance and a report. The results are included with the enterprise risk assessment which is communicated to the board and executive level managers annually.
		Atlassian has established a Whistleblower hotline that is accessible to both external individuals and employees within the Company.
		Vendor agreements, including any security, availability and confidentiality commitments, are reviewed by appropriate Atlassian management during the procurement process.
		Atlassian reviews the SOC reports of the vendors on an annual basis.
		Customer terms of service are standardized and approved by legal. The terms of service communicate the security, availability and confidentiality commitments to the customer and any changes are communicated.
		Users may report bugs, defects, or availability, security and confidentiality issues.
		Customer responsibilities are described on the Trello customer-facing website.
		A description of the system delineating the boundaries and describing relevant components is documented on the Atlassian intranet and the customer-facing website.
		Atlassian communicates its commitment to security as a top priority for its customers via Atlassian Trust Security page.
		Atlassian communicates changes to confidentiality commitments through Atlassian's web site, when applicable.

Common Criteria (CC) to All Security, Availability, and Confidentiality Principles
CC2.0 Common Criteria Related to Control Environment

CC	Criteria	Controls of Atlassian
CC2.3 (Cont.)		Significant changes made to the system are communicated to internal users and customers.
		Availability is published so that Customers may check the status/uptime of Trello.
		Monitoring tools are in place to track and notify on the availability of Trello systems and services.

Common Criteria (CC) to All Security, Availability and Confidentiality Principles
CC3.0 Common Criteria Related to Risk Assessment

CC	Criteria	Controls of Atlassian
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Atlassian has defined an ERM process and conducts an enterprise risk assessment on an annual basis, which includes key product stakeholders.
		The Atlassian Risk and Compliance team evaluates the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Atlassian maintains a risk and controls matrix within their GRC tool.
		The Atlassian Risk and Compliance team monitors the environment of internal control and identifies significant changes that have occurred.
		Internal audits are performed, results are communicated and corrective actions monitored.
		At least annually, the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) review committee charters and corporate governance which define their roles, responsibilities, meeting frequency, participants, and member qualifications.
		A fraud risk assessment is performed annually by the Head of Risk and Compliance. A cross-functional survey of employees in areas susceptible to fraud is conducted and combined with an evaluation of external risks. Results are evaluated by the Head of Risk and Compliance and a report. The results are included with the enterprise risk assessment which is communicated to the board and executive level managers annually.
		Financial statement risk assessment performed by Internal Audit and reviewed by Controller.
		Annually, a standard disclosure checklist is completed by a member of Technical Accounting to identify areas for disclosure. The Head of Technical Accounting & Financial Reporting reviews an electronic copy of the checklist for completeness and accuracy of

Common Criteria (CC) to All Security, Availability and Confidentiality Principles
CC3.0 Common Criteria Related to Risk Assessment

CC	Criteria	Controls of Atlassian
CC3.1 (Cont.)		responses provided and evidences review and approval via JIRA Service Desk.
		The Corporate Controller reviews the financials and footnote disclosures prepared by the member of Technical Accounting for reasonableness, internal consistency and confirms prior period balances of the final financial statements. A copy of the reviewed statements is attached to an email to the CFO evidencing completion of review.
		The signature authority matrix is maintained by Legal which establishes the signature authority for expenditures, contracts, capital acquisitions and write offs. Separately, the Corporate Controller established the cash disbursement.
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.	Atlassian has defined an ERM process and conducts an enterprise risk assessment on an annual basis, which includes key product stakeholders.
		The Atlassian Risk and Compliance team evaluates the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Atlassian maintains a risk and controls matrix within their GRC tool.
		The Atlassian Risk and Compliance team monitors the environment of internal control and identifies significant changes that have occurred.
		Internal audits are performed, results are communicated, and corrective actions are monitored.
		A fraud risk assessment is performed annually by the Head of Risk and Compliance. A cross-functional survey of employees in areas susceptible to fraud is conducted and combined with an evaluation of external risks. Results are evaluated by the Head of Risk and Compliance and a report. The results are included with the enterprise risk assessment which is communicated to the board and executive level managers annually.
		An organizational wide incident management process is in place, with the SRE team

Common Criteria (CC) to All Security, Availability and Confidentiality Principles
CC3.0 Common Criteria Related to Risk Assessment

CC	Criteria	Controls of Atlassian
CC3.2 (Cont.)		responsible for incidents and problems for Atlassian services and platforms. Incident management process must meet the Atlassian Incident Management Standard.
		Malware protection is implemented and security patching is enforced on Windows endpoints.
		Penetration testing is performed by Bug Bounty on a continuous basis. Issues are reviewed and tracked to completion in a JIRA ticket timely.
		Monitoring tools are in place to track and notify on the availability of Trello systems and services
		Technical vulnerability management is implemented using vulnerability scanners. Critical threats are reviewed and resolved timely.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	A fraud risk assessment is performed annually by the Head of Risk and Compliance. A cross-functional survey of employees in areas susceptible to fraud is conducted and combined with an evaluation of external risks. Results are evaluated by the Head of Risk and Compliance and a report. The results are included with the enterprise risk assessment which is communicated to the board and executive level managers annually.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	Audit Committee Charter defines roles, responsibilities and key activities.
		Audit Committee Meeting calendar and general meeting agenda are developed.
		Qualifications for the Audit Committee's "Financial Expert" have been defined in the audit committee charter.
		The Atlassian Risk and Compliance team evaluates the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Atlassian maintains a risk and controls matrix within their GRC tool.
		The Atlassian Risk and Compliance team monitors the environment of internal control and identifies significant changes that have occurred.
		Vendor agreements, including any security, availability and confidentiality commitments,

Common Criteria (CC) to All Security, Availability and Confidentiality Principles
CC3.0 Common Criteria Related to Risk Assessment

CC	Criteria	Controls of Atlassian
CC3.4 (Cont.)		are reviewed by appropriate Atlassian management during the procurement process.

Common Criteria (CC) to All Security, Availability and Confidentiality Principles
CC4.0 Common Criteria Related to Monitoring Activities

CC	Criteria	Controls of Atlassian
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.	Atlassian has defined an ERM process and conducts an enterprise risk assessment on an annual basis, which includes key product stakeholders.
		The Atlassian Risk and Compliance team evaluates the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Atlassian maintains a risk and controls matrix within their GRC tool.
		The Atlassian Risk and Compliance team monitors the environment of internal control and identifies significant changes that have occurred.
		Internal audits are performed, results are communicated, and corrective actions are monitored.
		At least annually, the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) review committee charters and corporate governance which define their roles, responsibilities, meeting frequency, participants, and member qualifications.
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.	Atlassian has defined an ERM process and conducts an enterprise risk assessment on an annual basis, which includes key product stakeholders.
		The Atlassian Risk and Compliance team evaluates the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Atlassian maintains a risk and controls matrix within their GRC tool.
		The Atlassian Risk and Compliance team monitors the environment of internal control and identifies significant changes that have occurred.
		Internal audits are performed, results are communicated, and corrective actions are monitored.

Common Criteria (CC) to All Security, Availability and Confidentiality Principles

CC4.0 Common Criteria Related to Monitoring Activities

CC	Criteria	Controls of Atlassian
CC4.2 (Cont.)		At least annually, the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) review committee charters and corporate governance which define their roles, responsibilities, meeting frequency, participants, and member qualifications.

Common Criteria (CC) to All Security, Availability and Confidentiality Principles

CC5.0 Common Criteria Related to Control Activities

CC	Criteria	Controls of Atlassian
CC5.1	The entity selects and develops control activities that contribute to the migration of risks to the achievement of objectives to acceptable levels.	Atlassian has defined an ERM process and conducts an enterprise risk assessment on an annual basis, which includes key product stakeholders.
		The Atlassian Risk and Compliance team evaluates the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Atlassian maintains a risk and controls matrix within their GRC tool.
		The Atlassian Risk and Compliance team monitors the environment of internal control and identifies significant changes that have occurred.
		Internal audits are performed, results are communicated, and corrective actions are monitored.
		A fraud risk assessment is performed annually by the Head of Risk and Compliance. A cross-functional survey of employees in areas susceptible to fraud is conducted and combined with an evaluation of external risks. Results are evaluated by the Head of Risk and Compliance and a report. The results are included with the enterprise risk assessment which is communicated to the board and executive level managers annually.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Atlassian has defined an ERM process and conducts an enterprise risk assessment on an annual basis, which includes key product stakeholders.
		The Atlassian Risk and Compliance team evaluates the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Atlassian maintains a risk and controls matrix within their GRC tool.
		The Atlassian Risk and Compliance team monitors the environment of internal control and identifies significant changes that have occurred.

Common Criteria (CC) to All Security, Availability and Confidentiality Principles
CC5.0 Common Criteria Related to Control Activities

CC	Criteria	Controls of Atlassian
CC5.2 (Cont.)		Internal audits are performed, results are communicated, and corrective actions are monitored.
		At least annually, the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) review committee charters and corporate governance which define their roles, responsibilities, meeting frequency, participants, and member qualifications.
		A fraud risk assessment is performed annually by the Head of Risk and Compliance. A cross-functional survey of employees in areas susceptible to fraud is conducted and combined with an evaluation of external risks. Results are evaluated by the Head of Risk and Compliance and a report. The results are included with the enterprise risk assessment which is communicated to the board and executive level managers annually.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Atlassian has defined an ERM process and conducts an enterprise risk assessment on an annual basis, which includes key product stakeholders.
		The Atlassian Risk and Compliance team evaluates the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Atlassian maintains a risk and controls matrix within their GRC tool.
		The Atlassian Risk and Compliance team monitors the environment of internal control and identifies significant changes that have occurred.
		Internal audits are performed, results are communicated, and corrective actions are monitored.
		Policies are posted and available online, assigned a policy owner, and reviewed by appropriate Atlassian management at least annually.

Common Criteria (CC) to All Security, Availability and Confidentiality Principles
CC5.0 Common Criteria Related to Control Activities

CC	Criteria	Controls of Atlassian
CC5.3 (Cont.)		Candidates are reviewed and approved by at least two interviewers prior to hiring.
		Performance appraisals are performed at least annually.
		Training is provided to employees to support their continued development and growth.

Common Criteria (CC) to All Security, Availability and Confidentiality Principles

CC6.0 Common Criteria Related to Logical and Physical Access Controls

CC	Criteria	Controls of Atlassian
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 logging into VPN (Remote Access Service) from any IP address.
		Duo integrates with Centrify to require two-factor authentication. Duo also extends two-factor protection to applications launched from a Centrify browser session. Duo two-factor authentication is required when logging in from any IP that is not whitelisted within the "exempt IP" settings in Centrify.
		Direct access to the Trello Platform via Jumpbox requires a valid SSH key and two factor authentication.
		Access to the Atlassian internal network and internal tools is restricted to authorized users via logical access measures: • Each Atlassian user must have an active Active Directory account • Each Atlassian user must be members of the appropriate LDAP group
		Active Directory group membership is automatically assigned based on the user's department and team.
		Active customers use authentication and authorization methods that meet password length of 8 characters.
		Centrify single sign-on allows users to have a single point of authentication to access multiple applications. Centrify enforces minimum password length configured in Active Directory.
		Privileged access to Deployment Bamboo is restricted to the members of the Build Engineering team.
		Privileged access to Trello services are formally requested and approved prior to being provisioned.
		An automatic alert is triggered to the Risk and Compliance Manager and HR For any role change between the following groups: Engineering, Support, or Finance group. Appropriateness of access is reviewed and approved.

Common Criteria (CC) to All Security, Availability and Confidentiality Principles
CC6.0 Common Criteria Related to Logical and Physical Access Controls

CC	Criteria	Controls of Atlassian
CC6.1 (Cont.)		Managers enter termination dates into Workday prior to the termination.
		The HR system does not allow terminations to be backdated.
		Within up to 8 hours of a user account being marked as inactive in Workday, user accounts are suspended in Centrify and Active Directory, including being removed from associated Active Directory groups. User access to the network is also disabled once users are terminated. Once terminated via the above process, users are unable to manually connect to the network, login to the Wi-Fi or access via VPN, including remote access via Duo.
		Within up to 12 hours of a user account being marked as inactive in Workday, user accounts are suspended in Centrify and Active Directory. Once suspended, users are unable to access Trello's systems, as all access to Trello's systems requires the user to be on the Atlassian network. Any access to systems whose privileges are not managed by AD/Centrify/Workday/Google Authentication will be revoked manually by an administrator per the Trello SOP - Staff Transfer and Termination page.
		The People Central Systems Support Specialist performs a review over Workday admin users semi-annually.
		User access reviews for access to Trello services are performed and completed in a timely manner.
		The Build Engineering Development Team Lead performs a review of privileged user access for deployment-bamboo semi-annually.
		Access to customer data by the Trello Support team is supported by a valid customer support request.
		External users securely connect to Trello via the encrypted TLS protocol.

Common Criteria (CC) to All Security, Availability and Confidentiality Principles
CC6.0 Common Criteria Related to Logical and Physical Access Controls

CC	Criteria	Controls of Atlassian
CC6.1 (Cont.)		Trello media attachment contents are encrypted.
		Malware protection is implemented and security patching is enforced on Windows endpoints.
		IT Asset management software is used to monitor hard drive encryption, user authentication requirements, and security patching on MacOS endpoints.
		Atlassian reviews the SOC reports of the third-party vendors on an annual basis.
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.	Two-factor authentication is required when logging into VPN (Remote Access Service) from any IP address.
		Centrify single sign-on allows users to have a single point of authentication to access multiple applications. Centrify enforces minimum password length configured in Active Directory.
		Access to the Atlassian internal network and internal tools is restricted to authorized users via logical access measures: • Each Atlassian user must have an active Active Directory account • Each Atlassian user must be members of the appropriate LDAP group
		Direct access to the Trello Platform via Jumpbox requires a valid SSH key and two factor authentication.
		Active customers use authentication and authorization methods that meet password length of 8 characters.
		Privileged access to Deployment Bamboo is restricted to the members of the Build Engineering team.
		Privileged access to Trello services are formally requested and approved prior to being provisioned.
		An automatic alert is triggered to the Risk and Compliance Manager and HR for any role change between the following groups: Engineering, Support, or Finance group. Appropriateness of access is reviewed and approved.

Common Criteria (CC) to All Security, Availability and Confidentiality Principles
CC6.0 Common Criteria Related to Logical and Physical Access Controls

CC	Criteria	Controls of Atlassian
CC6.2 (Cont.)		Managers enter termination dates into Workday prior to the termination.
		The HR system does not allow terminations to be backdated.
		Within up to 8 hours of a user account being marked as inactive in Workday, user accounts are suspended in Centrify and Active Directory, including being removed from associated Active Directory groups. User access to the network is also disabled once users are terminated. Once terminated via the above process, users are unable to manually connect to the network, login to the Wi-Fi or access via VPN, including remote access via Duo.
		Within up to 12 hours of a user account being marked as inactive in Workday, user accounts are suspended in Centrify and Active Directory. Once suspended, users are unable to access Trello's systems, as all access to Trello's systems requires the user to be on the Atlassian network. Any access to systems whose privileges are not managed by AD/Centrify/Workday/Google Authentication will be revoked manually by an administrator per the Trello SOP - Staff Transfer and Termination page.
		The People Central Systems Support Specialist performs a review over Workday admin users semi-annually.
		User access reviews for access to Trello services are performed and completed in a timely manner.
		The Build Engineering Development Team Lead performs a review of privileged user access for deployment-bamboo semi-annually.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets	Direct access to the Trello Platform via Jumpbox requires a valid SSH key and two factor authentication.
		Access to the Atlassian internal network and

Common Criteria (CC) to All Security, Availability and Confidentiality Principles
CC6.0 Common Criteria Related to Logical and Physical Access Controls

CC	Criteria	Controls of Atlassian
CC6.3 (Cont.)	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.	internal tools is restricted to authorized users via logical access measures: • Each Atlassian user must have an active Active Directory account • Each Atlassian user must be members of the appropriate LDAP group
		Active Directory group membership is automatically assigned based on the user's department and team.
		Privileged access to Deployment Bamboo is restricted to the members of the Build Engineering team.
		Privileged access to Trello services are formally requested and approved prior to being provisioned.
		Within up to 12 hours of a user account being marked as inactive in Workday, user accounts are suspended in Centrify and Active Directory. Once suspended, users are unable to access Trello's systems, as all access to Trello's systems requires the user to be on the Atlassian network. Any access to systems whose privileges are not managed by AD/Centrify/Workday/Google Authentication will be revoked manually by an administrator per the Trello SOP - Staff Transfer and Termination page.
		An automatic alert is triggered to the Risk and Compliance Manager and HR For any role change between the following groups: Engineering, Support, or Finance group. Appropriateness of access is reviewed and approved.
		The People Central Systems Support Specialist performs a review over Workday admin users semi-annually.
		User access reviews for access to Trello services are performed and completed in a timely manner.

Common Criteria (CC) to All Security, Availability and Confidentiality Principles
CC6.0 Common Criteria Related to Logical and Physical Access Controls

CC	Criteria	Controls of Atlassian
CC6.3 (Cont.)		The Build Engineering Development Team Lead performs a review of privileged user access for deployment-bamboo semi-annually.
		Access to customer data by the Trello Support team is supported by a valid customer support request.
CC6.4	The entity restricts physical access to facilities and protected information assets (For example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Atlassian reviews the SOC reports of the third-party vendors on an annual basis.
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.	Atlassian reviews the SOC reports of the third-party vendors on an annual basis.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Two-factor authentication is required when logging into VPN (Remote Access Service) from any IP address.
		Duo integrates with Centrify to require two-factor authentication. Duo also extends two-factor protection to applications launched from a Centrify browser session. Duo two-factor authentication is required when logging in from any IP that is not whitelisted within the "exempt IP" settings in Centrify.
		Direct access to the Trello Platform via Jumpbox requires a valid SSH key and two factor authentication.
		Access to the Atlassian internal network and internal tools is restricted to authorized users via logical access measures: • Each Atlassian user must have an active Active Directory account • Each Atlassian user must be members of

Common Criteria (CC) to All Security, Availability and Confidentiality Principles
CC6.0 Common Criteria Related to Logical and Physical Access Controls

CC	Criteria	Controls of Atlassian
CC6.6 (Cont.)		the appropriate LDAP group
		External users securely connect to Trello via the encrypted TLS protocol.
		Firewall rules are in place to restrict access to the Trello production environment.
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.	External users securely connect to Trello via the encrypted TLS protocol.
		Trello assigns unique identifiers upon creation to customer data.
		Protection of prod data in non-prod environments.
		Trello data is deleted within 90 days of receipt of a request for deletion.
		Trello media attachment contents are encrypted.
		Malware protection is implemented and security patching is enforced on Windows endpoints.
		IT Asset management software is used to monitor hard drive encryption, user authentication requirements, and security patching on MacOS endpoints.
		Firewall rules are in place to restrict access to the Trello production environment.
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.	Peer review and passed green build testing is required prior to merging the code to the production branch.
		Bitbucket does not allow change pull request to be approved by the same user who requests it.
		Bamboo will not allow code to be deployed unless it has passed green build testing. A green build (successful build) occurs when all the tests as defined within the Bamboo build plan have successfully completed. A red build occurs if any tests defined within the Bamboo build plan fail.
		Deployment Bamboo performs a check to validate that the SOX setting on Bitbucket are compliant to following: * Requires >1 approver * Unapprove automatically on new changes * Changes without a pull request

Common Criteria (CC) to All Security, Availability and Confidentiality Principles
CC6.0 Common Criteria Related to Logical and Physical Access Controls

CC	Criteria	Controls of Atlassian
CC6.8 (Cont.)		If the settings are not enforced, the code is rejected.
		Trello will not allow code artifacts to deploy or run on the platform unless they have been peer reviewed and have passed green build testing.
		Operating system, database, Puppet, deployment script, and emergency changes follow the same process as the application changes.
		Privileged access to Deployment Bamboo is restricted to the members of the Build Engineering team.
		A JIRA ticket is automatically generated if a change to the enforcement of peer review/pull requests occurs.
		Malware protection is implemented and security patching is enforced on Windows endpoints.
		IT Asset management software is used to monitor hard drive encryption, user authentication requirements, and security patching on MacOS endpoints.
		Users may report bugs, defects, or availability, security and confidentiality issues.
		An organizational wide incident management process is in place, with the SRE team responsible for incidents and problems for Atlassian services and platforms. Incident management process must meet the Atlassian Incident Management Standard
		Code scanning is performed by SourceClear on a continuous basis for Trello.

Common Criteria (CC) to All Security, Availability and Confidentiality Principles
CC7.0 Common Criteria Related to System Operations

CC	Criteria	Controls of Atlassian
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.	Code scanning is performed by SourceClear on a continuous basis for Trello.
		Penetration testing is performed by Bug Bounty on a continuous basis. Issues are reviewed and tracked to completion in a JIRA ticket timely.
		Monitoring tools are in place to track and notify on the availability of Trello systems and services.
		Technical vulnerability management is implemented using vulnerability scanners. Critical threats are reviewed and resolved timely.
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 analysed to determine whether they represent security events.	Penetration testing is performed by Bug Bounty on a continuous basis. Issues are reviewed and tracked to completion in a JIRA ticket timely.
		Monitoring tools are in place to track and notify on the availability of Trello systems and services.
		Technical vulnerability management is implemented using vulnerability scanners. Critical threats are reviewed and resolved timely.
		An organizational wide incident management process is in place, with the SRE team responsible for incidents and problems for Atlassian services and platforms. Incident management process must meet the Atlassian Incident Management Standard.
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, take actions to prevent or address such failures.	Penetration testing is performed by Bug Bounty on a continuous basis. Issues are reviewed and tracked to completion in a JIRA ticket timely.
		Technical vulnerability management is implemented using vulnerability scanners. Critical threats are reviewed and resolved timely.
		An organizational wide incident management process is in place, with the SRE team responsible for incidents and problems for Atlassian services and platforms. Incident management process must meet the Atlassian Incident Management Standard.

Common Criteria (CC) to All Security, Availability and Confidentiality Principles
CC7.0 Common Criteria Related to System Operations

CC	Criteria	Controls of Atlassian
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.	Policies are posted and available online, assigned a policy owner, and reviewed by appropriate Atlassian management at least annually.
		Atlassian communicates its commitment to security as a top priority for its customers via Atlassian Trust Security page.
		Penetration testing is performed by Bug Bounty on a continuous basis. Issues are reviewed and tracked to completion in a JIRA ticket timely.
		Technical vulnerability management is implemented using vulnerability scanners. Critical threats are reviewed and resolved timely.
		An organizational wide incident management process is in place, with the SRE team responsible for incidents and problems for Atlassian services and platforms. Incident management process must meet the Atlassian Incident Management Standard
		Users may report bugs, defects, or availability, security and confidentiality issues.
		A disaster recovery policy is in place and is reviewed on an annual basis by the disaster recovery steering committee.
		A disaster recovery plan is in place for Trello and its services which is tested on a quarterly basis. Key stakeholders are involved in the planning, impact analysis, execution, and remediation (if required).
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Atlassian communicates its commitment to security as a top priority for its customers via Atlassian Trust Security page.
		An organizational wide incident management process is in place, with the SRE team responsible for incidents and problems for Atlassian services and platforms. Incident management process must meet the Atlassian Incident Management Standard.
		Users may report bugs, defects, or availability, security and confidentiality issues.
		Trello performs frequent, automatic backups and routine restore testing.

Common Criteria (CC) to All Security, Availability and Confidentiality Principles
CC7.0 Common Criteria Related to System Operations

CC	Criteria	Controls of Atlassian
CC7.5 (Cont.)		A disaster recovery policy is in place and is reviewed on an annual basis by the disaster recovery steering committee.
		A disaster recovery plan is in place for Trello and its services which is tested on a quarterly basis. Key stakeholders are involved in the planning, impact analysis, execution, and remediation (if required).

Common Criteria (CC) to All Security, Availability and Confidentiality Principles
CC8.0 Common Criteria Related to Change Management

CC	Criteria	Controls of Atlassian
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.	Peer review and passed green build testing is required prior to merging the code to the production branch.
		Bitbucket does not allow change pull request to be approved by the same user who requests it.
		Bamboo will not allow code to be deployed unless it has passed green build testing. A green build (successful build) occurs when all the tests as defined within the Bamboo build plan have successfully completed. A red build occurs if any tests defined within the Bamboo build plan fail.
		Deployment Bamboo performs a check to validate that the SOX setting on Bitbucket are compliant to following: * Requires >1 approver * Unapprove automatically on new changes * Changes without a pull request If the settings are not enforced, the code is rejected.
		Trello will not allow code artifacts to deploy or run on the platform unless they have been peer reviewed and have passed green build testing.
		Operating system, database, Puppet, deployment script, and emergency changes follow the same process as the application changes.
		Privileged access to Deployment Bamboo is restricted to the members of the Build Engineering team.

Common Criteria (CC) to All Security, Availability and Confidentiality Principles
CC9.0 Common Criteria Related to Risk Mitigation

CC	Criteria	Controls of Atlassian
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Atlassian has defined an ERM process and conducts an enterprise risk assessment on an annual basis, which includes key product stakeholders.
		The Atlassian Risk and Compliance team evaluates the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Atlassian maintains a risk and controls matrix within their GRC tool.
		The Atlassian Risk and Compliance team monitors the environment of internal control and identifies significant changes that have occurred.
		A disaster recovery policy is in place and is reviewed on an annual basis by the disaster recovery steering committee.
		A disaster recovery plan is in place for Trello and its services which is tested on a quarterly basis. Key stakeholders are involved in the planning, impact analysis, execution, and remediation (if required).
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Vendor agreements, including any security, availability and confidentiality commitments, are reviewed during the procurement process.
		Atlassian reviews the SOC reports of the third-party vendors on an annual basis.

Common Criteria (CC) to All Security, Availability and Confidentiality Principles
A1.0 Additional Criteria for Availability

CC	Criteria	Controls of Atlassian
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.	Monitoring tools are in place to track and notify on the availability of Trello systems and services. Availability is published so that Customers may check the status/uptime of Trello. Trello performs quarterly system-wide capacity audits.
A1.2	The entity authorizes, designs, develops or acquires, implements operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	Trello performs frequent, automatic backups and routine restore testing. A disaster recovery policy is in place and is reviewed on an annual basis by the disaster recovery steering committee. A disaster recovery plan is in place for Trello and its services which is tested on a quarterly basis. Key stakeholders are involved in the planning, impact analysis, execution, and remediation (if required). Atlassian reviews the SOC reports of the third-party vendors on an annual basis.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	Trello performs frequent, automatic backups and routine restore testing. A disaster recovery plan is in place for Trello and its services which is tested on a quarterly basis. Key stakeholders are involved in the planning, impact analysis, execution, and remediation (if required).

Common Criteria (CC) to All Security, Availability and Confidentiality Principles

C1.0 Additional Criteria for Confidentiality

CC	Criteria	Controls of Atlassian
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Data is classified according to company policy.
		Trello media attachment contents are encrypted.
		Production data is not used in non-production environments.
		External users securely connect to Trello via the encrypted TLS protocol.
		Trello assigns unique identifiers upon creation to customer data.
		Trello data is deleted within 90 days of receipt of a request for deletion.
		Vendor agreements, including any security, availability and confidentiality commitments, are reviewed by appropriate Atlassian management during the procurement process.
		Atlassian reviews the SOC reports of the third-party vendors on an annual basis.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	Data is classified according to company policy.
		Trello data is deleted within 90 days of receipt of a request for deletion.
		Vendor agreements, including any security, availability and confidentiality commitments, are reviewed by appropriate Atlassian management during the procurement process.
		Atlassian reviews the SOC reports of the third-party vendors on an annual basis.

SECTION V: OTHER INFORMATION PROVIDED BY ATLASSIAN

Other Information Provided by Atlassian

Atlassian offers multiple collaboration software and cloud products which allows the integration of various departments and management groups for both individuals and enterprises, as well as the visibility of the day to day project management activities for all users.

Atlassian takes the privacy and confidentiality of customers, and the integrity of their products, extremely seriously. The Company is committed to devoting the necessary resources to ensure the security of all customer information, and continuously update and strengthen their systems and processes against unauthorized access. The Company has security controls, such as bug bounty program, to detect security incidents that exist or have occurred within the Company's environment. In the event where an incident is identified, immediate action is taken to resolve the matter within the same day, or even within hours upon notification. As part of the investigation process, the following actions are performed:

- Incident tickets are created to document the timeline of the incident, details of the incident (including any data that was exposed), and immediate actions to mitigate and/or resolve the issue. All relevant data is further examined and documented in a timely manner.

- As part of the mitigation plan, the security team performs a root cause analysis to assess the materiality and impact of the incident. Assessment of the incident includes assessing the nature of the incident, the materiality of the data that is publicly exposed, the time period in which the data is exposed, any unauthorized access to the data, as well as impact towards all impacted customers and the Company itself.

- As part of the remediation process, the security team performs additional analysis to other potentially impacted environments to determine if the incident is isolated to a single product or environment. After an incident, the Company continues to monitor the situation to determine, among other things, if any complaints or litigation are filed by impacted customers.

- As part of the notification process, the legal team determines if any notification to the supervisory authorities and/or customers is required. The legal team evaluates all applicable laws, such as the General Data Protection Regulation ("GDPR") and state laws, as well as existing contractual agreements with impacted customers. Based on the evaluation of the incident, the legal team assess the nature and level of notification that is required.