Atlassian PTY Ltd.

System and Organization Controls (SOC) 2 Type 2 Report

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

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

With Independent Service Auditor's Assurance Report
including Tests Performed and Results Thereof

Table of Contents

Atlassian's Statuspage

Section I: Atlassian's Management Assertion For Statuspage

Atlassian's Management Assertion for Statuspage

We have prepared the accompanying Statuspage Description of System Relevant to Security, Availability and Confidentiality (Description) of Atlassian PTY Ltd ("Atlassian" or "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 Statuspage (System) that may be useful when assessing the risks arising from interactions with the System throughout the period November 1, 2019 to March 31, 2020, 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 Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

Atlassian uses Amazon Web Services ("AWS") and Heroku to provide physical safeguards, environmental safeguards, infrastructure support and management, and storage services. The organizations providing physical safeguards, environmental safeguards, infrastructure support and management, and storage services are collectively referred to as "Subservice Organizations". The Description includes only the controls of Atlassian and excludes controls of the Subservice Organizations. The Description also indicates that certain trust services criteria specified therein can be met only if the Subservice Organizations' controls assumed in the design of Atlassian's controls are suitably designed and operating effectively along with the related controls at the Service Organizations. The Description does not extend to controls of the Subservice Organizations.

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 throughout the period November 1, 2019 to March 31, 2020 in accordance with the Description Criteria.

b. The controls stated in the Description were suitably designed 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 throughout the period November 1, 2019 to March 31, 2020.

c. The Atlassian controls stated in the Description operated effectively throughout the period November 1, 2019 to March 31, 2020 to achieve the service commitments and system requirements based on the applicable trust services criteria, if user entities applied the complementary user entity controls and the subservice organizations applied the controls assumed in the design of Atlassian's controls throughout the period November 1, 2019 to March 31, 2020.

DocuSigned by:
8A8D3A5B24B14CD...
Erika Fisher
Chief Legal Officer, Atlassian

Section II: Independent Service Auditor's Report

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

Tel: +1 949 794 2300
Fax: +1 866 492 5140
ey.com

Building a better working world

Independent Service Auditor's Report

To the Management of Atlassian PTY Ltd.

Scope

We have examined Atlassian's accompanying Statuspage Description of System Relevant to Security, Availability, and Confidentiality (Description) of its Statuspage system used as an incident communication tool by organizations as part of their incident management process throughout the period November 1, 2019 to March 31, 2020 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 and operating effectiveness of controls included in the Description throughout the period November 1, 2019 to March 31, 2020 to provide reasonable assurance that the 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 Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

Atlassian uses Amazon Web Services ("AWS") and Heroku to provide physical safeguards, environmental safeguards, infrastructure support and management, and storage services. The organizations providing physical safeguards, environmental safeguards, infrastructure support and management, and storage services are collectively referred to as "Subservice Organizations". 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 Statuspage 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 implemented, suitably designed, and operating effectively at the Subservice Organizations. Our examination did not extend to the services provided by the Subservice Organizations and we have not evaluated whether the controls management assumes have been implemented at the Subservice Organizations have been implemented or whether such controls were suitably designed and operating effectively throughout the period November 1, 2019 to March 31, 2020.

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 operating effectively, 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.

Building a better working world

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's Management Assertion for Statuspage ("Assertion") about the presentation of the Description based on the Description Criteria and suitability of the design and operating effectiveness of the controls described therein to provide reasonable assurance that the service commitments and system requirements would be 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 and operating effectively 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 and operating effectiveness 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 and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria. 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 and operating effectiveness 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 controls stated in the Description are presented in accordance with the Description Criteria
- performing procedures to obtain evidence about whether controls stated in the Description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.

- assessing the risks that the Description is not presented in accordance with the Description Criteria and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria.
- testing the operating effectiveness of those controls based on the applicable trust services criteria.
- evaluating the overall presentation of the Description.

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

Inherent limitations
The Description is prepared to meet the common needs of a broad range of 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 provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness 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.

Description of tests of controls
The specific controls we tested and the nature, timing, and results of those tests are listed in the accompanying Atlassian's Controls and Service Auditor's Tests of Controls and Results of Tests (Description of Tests and Results).

Opinion
In our opinion, in all material respects:

a. the Description presents the Statuspage system that was designed and implemented throughout the period November 1, 2019 to March 31, 2020 in accordance with the Description Criteria.

b. the controls stated in the Description were suitably designed 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 effectively, and if the subservice organizations and user entities applied the controls assumed in the design of Atlassian's controls throughout the period November 1, 2019 to March 31, 2020.
c. the controls stated in the Description operated effectively to provide reasonable assurance that the service commitments and system requirements were achieved based on the applicable trust services criteria throughout the period November 1,

Building a better working world

2019 to March 31, 2020, if the subservice organization and user entity controls assumed in the design of Atlassian's controls operated effectively throughout the period November 1, 2019 to March 31, 2020.

Restricted use
This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of Atlassian, user entities of Atlassian's Statuspage system during some or all of the period November 1, 2019 to March 31, 2020, and prospective user entities, independent auditors and practitioners providing services to such user entities 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 service organization's service commitments and system requirements and how controls address those risks

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

Ernst & Young LLP

May 21, 2020
Irvine, California

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

Statuspage 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 Statuspage product (hereinafter "the System" or "Statuspage") for the period from November 1, 2019 to March 31, 2020 for the Security, Availability, and Confidentiality Trust Services Criteria.

The description is intended to provide Statuspage customers, prospective customers, and auditors with information about the system controls related to the criteria for the Security, Availability, and Confidentiality Trust Services Criteria 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 and operating effectiveness of the controls included in the Description throughout the period from November 1, 2019 to March 31, 2020 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 Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (applicable trust criteria)*. This description may not provide information about Atlassian's Statuspage 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, New York City, New York, Sydney, Australia, Manila, Philippines, Yokohama, Japan, Amsterdam, Netherlands, Austin, Texas, Boston, Massachusetts, Falls Church, Virginia, Ankara, Turkey, 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, Statuspage, Trello, Opsgenie, and Jira Align.

The system in-scope for this report is the Statuspage 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

Statuspage is an incident communication tool used by organizations as part of their incident management process. Statuspage provides a public or private facing page that allows companies to report on the status of any of their internal or external services. The product can also display relevant service metrics on the page. Customer users can subscribe to updates via SMS, email, or webhooks, so they can proactively be informed about incidents or updates the company has decided to communicate about. Statuspage is a Software as a Service ("SaaS") solution and only offered via the web.

Principal Service Commitments and System Requirements

Atlassian designs its processes and procedures to meet the objectives of the Statuspage system. Those objectives are based on the service commitments that Atlassian makes to user entities, the laws and regulations that govern the provision of the Statuspage system and the financial, operational, and compliance requirements that Atlassian has established for the system.

Security, availability, and confidentiality commitments to user entities are documented and communicated in the terms of services within the sign-up page in Statuspage and through the Master Service Agreement ("MSA") with other vendors and enterprise customers. The description of the service offering and the system delineating the boundaries and describing relevant components is documented on the Atlassian intranet and the customer-facing website. Security, availability, and confidentiality commitments are standardized and communicated to its customers via the Atlassian Trust Security Page. The security, availability, and confidentiality commitments include, but are not limited to, the following:

- Operational Practices — A range of security and confidentiality controls designed to address the security and confidentiality criteria of the Statuspage system. Such security and confidentiality controls include permitting and restricting system users to access customer data and the information they need based on their roles and responsibilities, while restricting them from accessing information not needed for their role.
- Product Security — A range of security controls Atlassian implements to keep the Statuspage system and customer's data safe. This includes the use of encryption technologies to protect customer data at rest and in transit, and formal processes to grant and revoke access to customer data.
- Reliability and Availability — Hosting data with Atlassian's cloud hosting partners while focusing on product resiliency to minimize downtime, as well as optimal performance with redundancy and failover options globally while maintaining multiple locations and availability zones across regions.
- Security Process — A range of vulnerability and security processes to detect security and vulnerability issues, which allows Atlassian to address identified gaps as soon as possible to minimize impact.

Atlassian establishes operational requirements that support the achievement of security, availability, and confidentiality commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Atlassian's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Statuspage system.

Infrastructure

Statuspage is hosted at Amazon Web Services ("AWS") data centers, using the AWS Infrastructure as a Service ("IaaS") offering. The services that make up the Statuspage

system are primarily isolated within a single large private network, which is spread out across multiple failure domains (or Availability Zones) for redundancy and fault-tolerance.

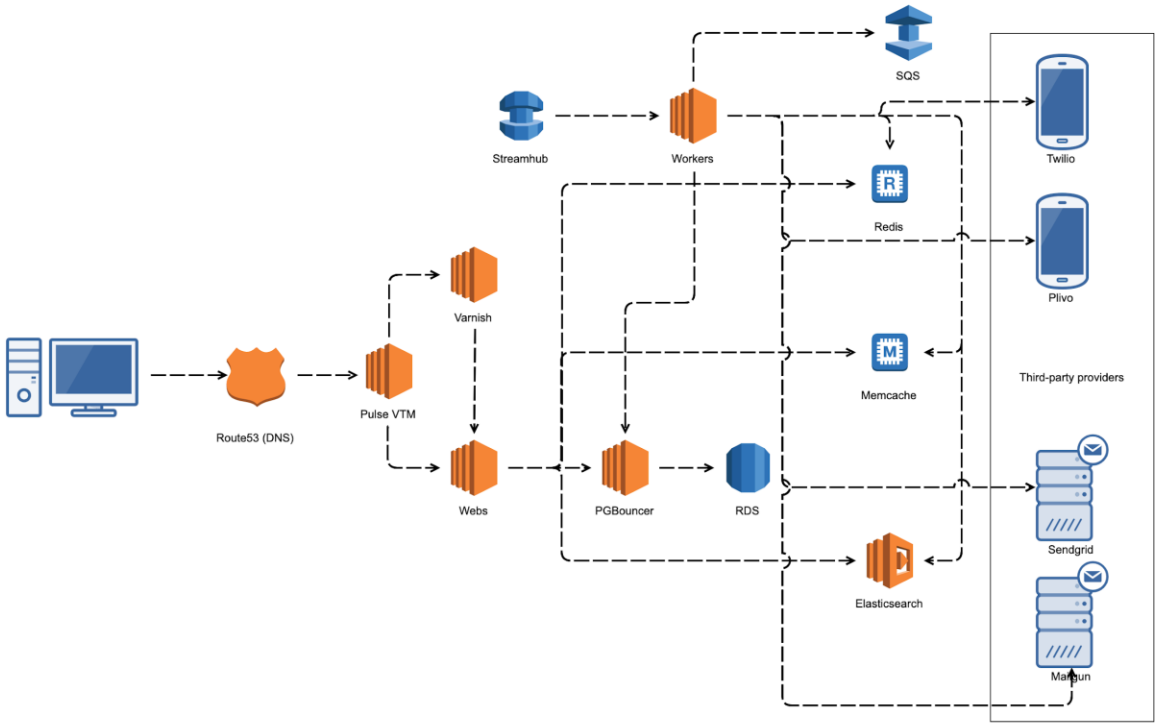

Figure 1: Statuspage's Infrastructure

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

- Data Storage: AWS RDS – Postgres stores customer data within Statuspage and AWS S3 stores attachments. All the application services interact with the database through "PgBouncer", an open source software that provides a proxying solution and is hosted in Atlassian's micros platform.
- Job Queue: AWS Elasticache Redis processes asynchronous jobs within the application (including notification delivery).
- Load Balancers and Network Connections: Pulse VTM, the load balancing solution, is spread across 4 different AWS regions (eu-west1, us-east1, us-west2, apse2). Route 53 stores the DNS hosted zones and has latency based routing enabled to forward traffic to the VTMs (based on user location).
- Indexing of Data: AWS Elasticsearch is used for indexing data for the purposes of search.
- Data Caching:
    1. Memcache is used for data caching and lookups on application side
    2. Varnish is used for caching static pages for customers

The processes and controls managed by AWS are excluded from the scope of this report. Atlassian manages the access to the database, configuration of the monitoring services, and backups of customer data. As such, these are in scope for this report.

Servers

AWS provides Infrastructure as a Service ("IaaS") and the initial creation of the virtual servers, which run Statuspage. The software and operating system configurations are managed by Atlassian's Micros team. Statuspage deploys all of its code via Atlassian's Micros Platform as a Service ("PaaS"). Statuspage manages their own datastores (Postgres, Redis, Memcached, and Elasticsearch) via AWS.

Database

Statuspage's primary datastore is an RDS cluster within the private network, which is hosted in AWS and managed by the Statuspage SRE Team. The RDS cluster includes a leader and multiple followers and its nodes are spread out across at least 3 Availability Zones for fault-tolerance and redundancy.

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

User attachments are stored within AWS S3 to increase durability, and to segregate attachments using a unique identifier that is stored in the Statuspage database. The unique identifier ties the file objects to the user.

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

Software

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

- Amazon Web Services ("AWS") – Cloud provider, cloud computing, database, file & messaging services, monitoring & alerting
- Bitbucket Cloud – Atlassian's developed source code and development projects tool
- Duo/Centrify – Single sign on service used for Atlassian
- Deployment Bamboo – Atlassian developed continuous integration tool used to perform automated testing and deployment activities
- https://Getsupport.atlassian.com ("GSAC") – Atlassian customer support and engagement tool
- GoogleAuth – Single sign on service used for Atlassian employees and contractors
- Heroku – Hosts the https://metastatuspage.com status reporting site
- Jira – Ticketing system used for incident management, user access provisioning, and change management process
- Lever – Hiring tool
- Nexpose – Vulnerability scanning tool
- Opsgenie – Atlassian's incident and alert management tool

- Pingdom – Alerting tool for monitoring availability
- SignalFX – Atlassian's 3rd party vendor used for system monitoring and alerting platform
- Slack – Collaboration or instant messaging tool
- Sourceclear - Software tool to identify vulnerabilities in 3rd-party libraries used by application code
- Splunk – Monitoring of security and availability tool
- Statuspage Admin Panel – Internal tool used by Statuspage staff to support customers; including impersonation
- Workday – Human Resource (HR) system; including performance feedback

AWS and Heroku are third-party vendors. Atlassian performs a review of the SOC 2 report for AWS and Heroku. The evaluation of the SOC 2 reports are performed and reviewed by the Risk and Compliance Team, which includes an assessment of complementary 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, Lever, Nexpose, Pingdom, SignalFX, Slack, Sourceclear, Splunk, and Workday are 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.

Bitbucket Cloud, Deployment Bamboo, https://getsupport.atlassian.com ("GSAC"), Jira, and Opsgenie are Atlassian managed tools and are in-scope for the controls discussed below.

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 Statuspage using the https://www.statuspage.io website. Upon accepting the terms and conditions, and completing the sign-up flow, a new database record and unique identifier are created in RDS - Postgres for that customer account and their organization. The unique ID is used thereafter for associating data with the specific organization. The data is logically separated from other users' and organizations' data using these unique ID's. All user created data are similarly assigned unique identifiers such that they can be correctly associated to users, pages, and organizations. Static assets such as JPEGs and java scripts that users upload to customize their content are uploaded to AWS S3 and are linked via unique identifiers within the database.

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

All production customer data is encrypted at rest within Atlassian's network, which is managed by AWS. AWS' SOC 2 report is reviewed at least annually by Atlassian. External

users connect to Statuspage using encryption via the SSL (TLS) protocol. 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:

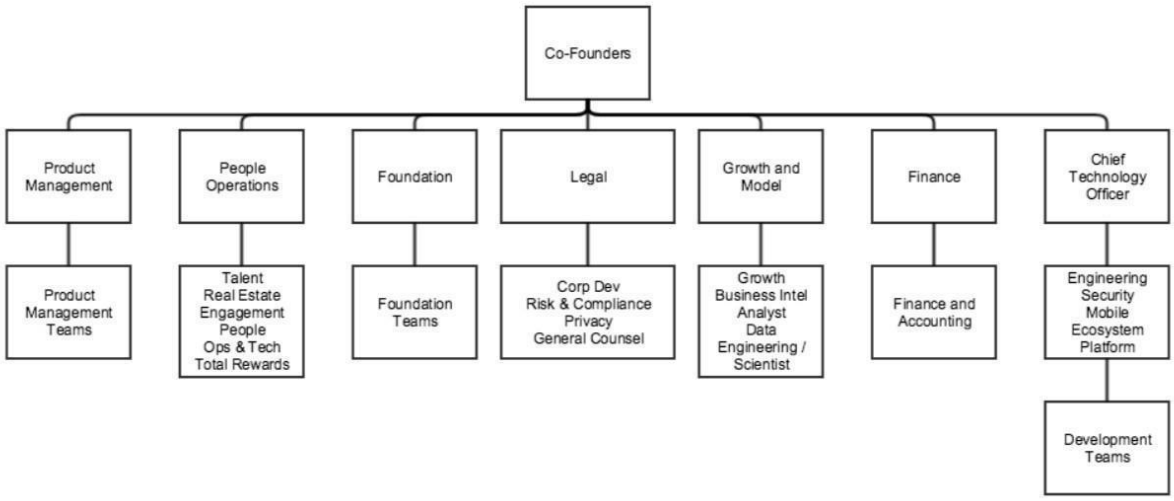

Figure 2: Atlassian's Organizational Chart

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

The Co-Founders are responsible for directing all designated areas including 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 hold them accountable.
        - Work with Recruitment to attract and hire outstanding individuals to create high performing balanced teams.
        - Lead by example and practice an inclusive management style.

Policies and Procedures

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

- Are properly communicated throughout the organization.
- Are properly owned, managed, and supported.
- Clearly outline business objectives.
- Show commitment to meet regulatory obligations.
- Are focused on continual iteration and improvement.
- Provide for an exception process.
- 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 a consistent outcome defined by the Standard or Guideline.

Policy Requirements

Every policy has a Policy Owner who is responsible for managing the risk outlined in the Policy Objective. All policies are reviewed, at least annually, to help ensure 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 will 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 Audit, 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 process of identifying and reviewing Board of Director candidates is defined in the Nominating and Governance Committee charter.

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. The audit committee charter includes the roles, responsibilities, key activities, and meetings. Qualifications for the audit committee's "Financial Expert" are also outlined and defined within the audit committee charter. The 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 practices, 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, 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, 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 regard 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.

Learning Central 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 Learning Central. 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, Get Abstract, Linkedin Learning, and Learndot are extensive third-party tools Atlassian uses to access thousands of online learning resources for free. It also

serves as the primary portals 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, interns, and graduates. 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. For interns and graduates, a recruiting manager will approve the offer letters because of the bulk nature and timing of these hires.

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 Workday (for check-ins and 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 relates 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 (ERM) process is modeled after ISO 31000-2009 "Risk Management — Principles and Guidelines".

An enterprise risk assessment is conducted on an annual basis, which includes key product stakeholders. 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 the 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 incidents.

- 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 engages with SMEs 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, skill sets, 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 tool. Links to detailed treatment plans, along with individual tasks are also established. The Risk and Compliance team monitors the progress and provides oversight of the plan's 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 monthly 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 evidence 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 are also reviewed and compared with other companies to determine the 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. The results are communicated and corrective actions are monitored to resolution. 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://Support.atlassian.com
- Social media
- General web site forms
- Email
- https://Community.atlassian.com
- https://Trust.atlassian.com
- Public bug site

Atlassian also communicates security, availability, and confidentiality criteria 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 Statuspage 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 Statuspage system, including the status and uptime, 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 include, 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 https://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 is 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 help raise 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 Statuspage platform and its supporting utilities and services are planned in Jira and Confluence Cloud 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. The Statuspage system also uses an internally developed platform-as-a-service ("PaaS"), which provides controlled, common solutions for micro-services such as deploying the service to machines, configuring load balancing, creating DNS records, etc.

Statuspage 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 changes 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 Statuspage 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 changes in the pull request must also pass automated tests that run in Atlassian's Deployment-Bamboo instance. Privileged access to Deployment Bamboo is limited 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.

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. Once confirmed, a docker image is built and tagged with the code's git hash. 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 and a Jira ticket is automatically generated for investigation. The tickets are automatically routed to the relevant development manager to confirm that no unauthorized changes were made, and to restore the setting.

The Statuspage production environment only accepts two types of builds: 1) builds that are signed by Deployment Bamboo or 2) builds that are from restricted folder where the artifacts are stored. Only Deployment Bamboo has access to push builds to the restricted folder and 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 Statuspage product. Major releases are also notified to customers through the customer-facing website.

Scanning of Production Code

Statuspage utilizes SourceClear to regularly scan and review the code base to detect vulnerable open source libraries being used. The scanner is integrated into the Statuspage build plan, and is run automatically when changes are made to the code base. Jira tickets are then manually created. Developers and Product Security 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 incident management ticket tracking system.

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.

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, meaning that change management controls are still adhered to.

B. Logical Access

Customer Production Accounts

Provisioning Customer Production Accounts

When creating an account with any of Atlassian's products, the user is directed to acknowledge the standardized customer agreement online. An account cannot be made for any of Atlassian's products without first being directed to acknowledge the customer agreement. 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 define 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 created. Users are all assigned unique identifiers upon creation of customer accounts, pages, and organizations, which are subsequently used by the Statuspage 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 in Statuspage (by the user themselves, or their organization's administrator in the case of enterprise accounts), all data regarding that user account is permanently erased within 30 days.

Customers can only request for their data to be deleted via a support ticket. Upon doing so, Support will validate the scope, timeframe, and legitimacy of the request, and if warranted, will facilitate the deletion. Support has crafted a set of tools to perform the deletion safely and consistently.

Production Environment Access

Customer Access

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

Users can access Statuspage via the browser user interface or using Statuspage's REST API.

User account authentication and management is handled within the Statuspage product. Users can authorize external services to access data using a user-specific API token. This token can be revoked and rotated via the Statuspage interface. Users can also subscribe to Statuspage updates via email, SMS, and webhook notifications based on incident and component status updates made within Statuspage.

Atlassian Internal Users Access

Access to Statuspage infrastructure is tightly restricted. All services are hosted within the production AWS account. Atlassian must authenticate through Atlassian's two-factor authentication via Duo 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 for AWS Console access. As for Micros (software and operating system) access, Atlassian users need to have a valid SSH key and can only access Micros services via Jumpbox.

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

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

Password

Customer Access

Statuspage customers are governed with a trial account when they first sign up. It is the customers' responsibility to ensure that their accounts are appropriately configured and set up to their individual or corporate network with other authentication mechanisms such as Single Sign-On ("SSO"), Google Auth, two-factor authentication, or strong password policies. SSO can be enabled for every user in the account for organizations on the Startup, or higher plan.

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 the Atlassian production environment. The primary method for connecting to Atlassian 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 8 characters is enforced for passwords in Centrify configured in Atlassian's Active Directory. Upon initial login, Atlassian employees can gain access to Google Suites (i.e. Gmail, Google Docs, Google Sheets, etc.) through GoogleAuth.

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. Active Directory group membership is automatically assigned based on the user's department and team.

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 Directory account
- Each Atlassian user account must be a member of the appropriate LDAP group

Access to the AWS production environment, Statuspage, and supporting tools, in addition to the Workday access group, 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 Jira ticket on the Statuspage Systems Access Request ("SSAR") project and appropriately reviewed and approved. Upon appropriate review and approval, access is provisioned, and the Jira ticket 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 (within up to 8 hours). 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 access to Statuspage's backend systems.

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 are 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 Statuspage 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

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

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

Vulnerability Scanning

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

- Technical vulnerability management is implemented using the Nexpose vulnerability scanners and Cloud Conformity Nexpose is used to run scans on the external and internal network, while Cloud Conformity is an AWS monitoring service used to scan configurations in AWS.
- Publicly identified vulnerabilities in Atlassian products are reported to Atlassian via the Atlassian Bug Bounty Program. This program is a vulnerability disclosure platform where security researchers can submit security issues for Atlassian's review.
- 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 uses vulnerability scanning tools to scan the internal and external-facing network, as well as configurations in AWS. 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 Statuspage 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 for malware protection. Ongoing workstation

asset management, security patch deployment, and drive encryption auditing is done using policies deployed through Active Directory (Windows) and Jamf Pro (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 place 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 is encrypted with the TLS cryptographic protocol. External users connect to Statuspage using encryption via the TLS protocol. Certificates are rotated when required.

C. Physical Access

Statuspage is hosted within AWS 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

A Capacity Planning program helps Atlassian determine what the current and future resource (people and technology) needs are in order to meet customer expectations of the goods and services being delivered. Statuspage performs capacity management on an ongoing, as well as scheduled basis. The infrastructure and systems that make up Statuspage are continuously monitored for utilization levels and adjusted accordingly. In addition to the constant resizing and reconfiguring of systems based on real-time load, Statuspage stakeholders conduct quarterly capacity 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.

Capacity planning is performed on a perpetual basis to help ensure projections are accurate and complete. Capacity planning is in place to better meet customer needs, help ensure compute and capacity resources are optimized, and to help forecast set capital expenditure.

E. Backup and Replication

Backups

Rolling live replicas of Statuspage's primary database are constantly being taken on a real-time basis (follower). Additionally, a full backup snapshot of the primary database is taken every day and is retained for up to 30 days.

Monitoring tools are used to monitor and identify data replication failure and latency, along with email alerts sent to the Statuspage SRE team for investigation and resolution.

Only authorized members of the Statuspage 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.

Full end-to-end backup restoration tests are performed semi-annually in the staging environment to simulate a production test and to ensure the team is trained and experienced with the process.

Replication

Statuspage utilizes a highly available cluster of RDS - Postgres servers within AWS to store data. It consists of 1 leader and 3 follower instances. These are deployed as multi-AZ instances to allow for maximum resiliency against underlying networking or availability issues within AWS.

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 both in the production and staging environments for Statuspage systems on a quarterly basis. Tabletop exercises are also performed to help 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 Statuspage 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 Statuspage 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 Statuspage engineering team aware of potential incidents such that they can be remediated before any customer-facing impact is realized. If needed, a HOT Ticket is created for these potential incidents that are resolved as part of the incident management process.

Statuspage uses tools to monitor the availability and processing capacity of customer-facing services. Changes to the availability of user-facing Statuspage services are published online so that customers may check the real-time and historical status of Statuspage 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 consist 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 the 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 has 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 HOT 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 (> 3% of customer data) • Hard service outage for more than 15 minutes
1	Critical incident with very high impact	Core functionality is affected for more than 5 minutes. Such as • Viewing, Updating Statuspage • CRUD for Incidents • Status updates for components • Notifications delay • Authentication • Data loss for customers (< 3 %)
2	Major incident with significant impact	Core functionality is affected but resolved in less than 5 minutes • Viewing, Updating Statuspage • CRUD for Incidents • Status updates for components • Notifications delay • Authentication This also includes some non-core functionalities that may be impacted for more than 30 minutes • Metrics • <=5 % spike in errors for status pages due to high volume of traffic Notifications via Twitter/Slack/Webhook
3	Minor incident with low impact	Non-core functionalities are affected • Metrics • Full text search • SSL deployments • Notifications via Twitter/Slack/Webhook • (The Rest of Management Portal) • Customer error pages • Full text search

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 – This assessment is made on the volume of customer tickets and % of traffic that is impaired or impacted.
- Customer/Internal service – Customer services such as https://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 products being slow might be a lot more impactful than a slow response from https://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 Statuspage components, system metrics, and a listing of past incidents: https://metastatuspage.com/history.

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 website
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 an 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

Complementary Subservice Organizations Controls

Atlassian utilizes subservice organizations to perform certain functions as described in the description above. Rather than duplicate the control tests, controls at Amazon Web Services and Heroku 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") and Heroku.

Criteria	Service Organization	Controls
CC6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Amazon Web Services (AWS) Heroku	IT access above least privileged, including administrator access, is approved by appropriate personnel prior to access provisioning. IT access privileges are reviewed on a quarterly basis by appropriate personnel. User access to systems is revoked timely upon termination. Data is encrypted in transit.
CC6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Amazon Web Services (AWS)	Physical access to the computer rooms, which house the entity's IT resources, servers, and related hardware, is restricted to authorized individuals through a badge access system or equivalent, and monitored by video surveillance. Requests for physical access privileges require management approval. Documented procedures exist for the identification and escalation of potential physical security breaches. Visitors must be signed in by an authorized workforce member before gaining entry and must be escorted at all times.
CC8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Amazon Web Services (AWS) Heroku	Changes are authorized, tested, and approved prior to implementation.

Criteria	Service Organization	Controls
A1.2: The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	Amazon Web Services (AWS) Heroku	Environmental protections have been installed including the following: ● Cooling systems ● Battery and generator backups ● Smoke detection ● Dry pipe sprinklers Environmental protection equipment receive maintenance on at least an annual basis.

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 Statuspage 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 Statuspage account.

Logical Access:

- Customers are responsible for creating a username and password to access their account.
- Customers are responsible for the safeguarding of their own account access credentials, including passwords or API keys and tokens.
- Customers are responsible for inviting team members and managing team members' access rights to Statuspage.
- Customers are responsible for establishing their own usage and access policies to their Statuspage 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, SSO, and GoogleAuth setup, if applicable.
- Customers are responsible for configuring the privacy and security settings of their own instance and Statuspage pages (i.e., private or public) according to their organization's policies and procedures.
- Customers are responsible for requesting, approving, and monitoring 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 Statuspage 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 having data classification policies relating to posting of information within their Statuspage pages.
- Customers are responsible for monitoring the confidentiality of data that is posted on their individual Statuspage pages.
- Customers are responsible for ensuring that their machines, devices, and network are secured.

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, availability, and confidentiality.

Section IV: Atlassian's Controls and Service Auditor's Tests of Controls and Results of Tests

Atlassian's Controls and Service Auditor's Tests of Controls and Results of Tests

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 and the tests performed by EY and results are the responsibility of the service auditor.

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 Security, Availability, and Confidentiality

CC 1.0 Common Criteria Related to Control Environment

CC 1.1 The entity demonstrates a commitment to integrity and ethical values.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Policies are posted and available online, assigned a policy owner, and reviewed at least annually by the designated policy owner or their delegate.	Inquired of the control owner and ascertained that policies were posted and available online, assigned a policy owner, and reviewed at least annually by the designated policy owner.	No deviation noted.
	Inspected the policies and ascertained that the policies were posted and available online, assigned a policy owner, and reviewed at least annually by the designated policy owner.	No deviation noted.
At least annually, the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) have annually reviewed committee charters and corporate governance which define their roles, responsibilities, meeting frequency, participants, member qualifications, and discussion topics.	Inquired of the control owner and ascertained that the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) reviewed committee charters and corporate governance which defined their roles, responsibilities, meeting frequency, participants, member qualifications on an annual basis.	No deviation noted.
	Inspected the current year's Board of Directors and subcommittee annual meeting minutes, and ascertained that committee charters and corporate governance, which defined their roles, responsibilities, meeting frequency, participants, and member qualifications, were discussed.	No deviation noted.
The process of identifying and reviewing Board of Director candidates is defined in Nominating and Governance Committee charter.	Inquired of the control owner and ascertained the process of identifying and reviewing Board of Director candidates was defined in Nominating and Governance Committee charter.	No deviation noted.
	Inspected the Nominating and Governance committee charter, and ascertained that the process of identifying and reviewing Board of Director candidates was defined.	No deviation noted.

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

CC 1.0 Common Criteria Related to Control Environment

CC 1.1 The entity demonstrates a commitment to integrity and ethical values.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
The Executive team sets strategic operational objectives annually.	Inquired of the control owner and ascertained the executive team sets Atlassian-level priorities annually.	No deviation noted.
	Inspected the Objectives and Key Results ("OKR") session minutes and ascertained that the executive team sets strategic operational objectives annually with each objective having an associated targeted results.	No deviation noted.
Employees and contractors acknowledge the Code of Conduct annually.	Inquired of the control owner and ascertained that employees as well as contractors, acknowledged the Code of Conduct annually.	No deviation noted.
	Inspected the code of conduct acknowledgement for a sample of active employees and contractors, and ascertained that employees as well as contractors acknowledged the Code of Conduct annually.	No deviation noted.
Performance appraisals are performed at least annually.	Inquired of the control owner and ascertained that performance appraisals were conducted at least annually.	No deviation noted.
	Inspected the performance appraisal results for a sample of employees and ascertained that performance appraisals were conducted at least annually.	The performance appraisals have not been performed during the audit period. The annual performance appraisals are performed between June and July annually. The last performance appraisals were performed in July 2019 and the next assessment

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

CC 1.0 Common Criteria Related to Control Environment

CC 1.1 The entity demonstrates a commitment to integrity and ethical values.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
		is expected to be completed in July 2020.
Vendor agreements, including any security, availability and confidentiality commitments, are reviewed during the procurement process.	Inquired of the control owner and ascertained that vendor agreements, including any security, availability, and confidentiality commitments, were reviewed during the procurement process.	No deviation noted.
	Inspected a sample of new vendors' third-party contracts and ascertained that the contracts included security, availability, and confidentiality commitments, and the contracts were executed between the third-party and Atlassian during the procurement process.	No deviation noted.

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

CC 1.0 Common Criteria Related to Control Environment

CC 1.2 The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
At least annually, the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) have annually reviewed committee charters and corporate governance which define their roles, responsibilities, meeting frequency, participants, member qualifications, and discussion topics.	Inquired of the control owner and ascertained that the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) reviewed committee charters and corporate governance which defined their roles, responsibilities, meeting frequency, participants, member qualifications on an annual basis.	No deviation noted.
	Inspected the current year's Board of Directors and subcommittee annual meeting minutes, and ascertained that committee charters and corporate governance, which defined their roles, responsibilities, meeting frequency, participants, and member qualifications, were discussed.	No deviation noted.
The process of identifying and reviewing Board of Director candidates is defined in Nominating and Governance Committee charter.	Inquired of the control owner and ascertained the process of identifying and reviewing Board of Director candidates was defined in Nominating and Governance Committee charter.	No deviation noted.
	Inspected the Nominating and Governance committee charter, and ascertained that the process of identifying and reviewing Board of Director candidates was defined.	No deviation noted.
Audit Committee Charter defines roles, responsibilities, and key activities of the audit committee.	Inquired of the control owner and ascertained that Audit Committee Charter defines roles, responsibilities, and key activities of the audit committee.	No deviation noted.
	Inspected the Audit Committee Charter in the Atlassian's website and ascertained that roles, responsibilities, and key activities of the audit committee were defined.	No deviation noted.

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

CC 1.0 Common Criteria Related to Control Environment

CC 1.2 The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Audit Committee meeting calendar and general meeting agenda are developed.	Inquired of the control owner and ascertained that Audit Committee meeting calendar and general meeting agendas were developed.	No deviation noted.
	Inspected the Audit Committee latest notice for the annual general meeting and ascertained that Audit Committee meeting calendar and general meeting agendas were developed.	No deviation noted.
Qualifications for the Audit Committee's "Financial Expert" have been defined in the audit committee charter.	Inquired of the control owner and ascertained that the Audit Committee Charter defined the qualifications for the Audit Committee's "Financial Expert".	No deviation noted.
	Inspected the Audit Committee Charter in the Atlassian's website and ascertained that qualifications for the "Financial Expert" was defined.	No deviation noted.
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.	Inquired of the control owner and ascertained that the Atlassian Risk and Compliance team evaluated the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Atlassian maintained a risk and controls matrix within their GRC tool.	No deviation noted.
	Inspected the GRC Tool used by Atlassian and ascertained that the Atlassian Risk and Compliance team evaluated the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Further ascertained that Atlassian maintained a risk and controls matrix within their GRC tool.	No deviation noted.

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

CC 1.0 Common Criteria Related to Control Environment

CC 1.3 Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
At least annually, the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) have annually reviewed committee charters and corporate governance which define their roles, responsibilities, meeting frequency, participants, member qualifications, and discussion topics.	Inquired of the control owner and ascertained that the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) reviewed committee charters and corporate governance which defined their roles, responsibilities, meeting frequency, participants, member qualifications on an annual basis.	No deviation noted.
	Inspected the current year's Board of Directors and subcommittee annual meeting minutes, and ascertained that committee charters and corporate governance, which defined their roles, responsibilities, meeting frequency, participants, and member qualifications, were discussed.	No deviation noted.
The process of identifying and reviewing Board of Director candidates is defined In Nominating and Governance Committee charter.	Inquired of the control owner and ascertained the process of identifying and reviewing Board of Director candidates was defined in Nominating and Governance Committee charter.	No deviation noted.
	Inspected the Nominating and Governance committee charter, and ascertained that the process of identifying and reviewing Board of Director candidates was defined.	No deviation noted.
Vendor agreements, including any security, availability and confidentiality commitments, are reviewed during the procurement process.	Inquired of the control owner and ascertained that vendor agreements, including any security, availability, and confidentiality commitments, were reviewed during the procurement process.	No deviation noted.
	Inspected a sample of new vendors' third-party contracts and ascertained that the contracts included security, availability, and confidentiality commitments, and the contracts were executed	No deviation noted.

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

CC 1.0 Common Criteria Related to Control Environment

CC 1.3 Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	between the third-party and Atlassian during the procurement process.	
Atlassian reviews the SOC report of the vendor on an annual basis.	Inquired of the control owner and ascertained that Atlassian reviewed the SOC reports of the vendors ("subservice organizations") on an annual basis.	No deviation noted.
	Inspected the Jira ticket for the review of the SOC 2 or equivalent attestation reports and ascertained that leadership reviewed the reports annually. Reviews included an assessment of complementary user entity controls, subservice organizations, and mapping of the controls to key risks. If there were exceptions, Atlassian reviewed the severity and impact of the exceptions, and if needed, followed-up with the individual vendor.	No deviation noted.
Hiring manager reviews and approves the job description prior to posting of job ads.	Inquired of the control owner and ascertained that hiring manager reviewed and approved the job description prior to posting of job ads.	No deviation noted.
	Inspected the configuration on Lever automation software and observed that it was configured to directly post job ads to the career page and respective job boards following approval from the respective hiring manager.	No deviation noted.
	Attempted to post a job ad to the career page without an approval and ascertained that the posting of job ads was rejected without appropriate approval.	No deviation noted.
	Inspected the hiring manager approvers for a sample of job ads posted and ascertained that the job descriptions for the job ads were reviewed and approved by the hiring manager prior to posting.	No deviation noted.

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

CC 1.0 Common Criteria Related to Control Environment

CC 1.3 Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Organizational charts are updated based on employee action notices and available to all Atlassian employees via Workday.	Inquired of the control owner and ascertained that organizational charts were updated based on employee action notices, and available to all Atlassian employees via Workday.	No deviation noted.
	Inspected the organization charts and ascertained that the organizational charts were updated based on employee action notices, and available to all Atlassian employees via Workday.	No deviation noted.
The organizational charts are reviewed by appropriate Atlassian management and updated semi-annually.	Inquired of the control owner and ascertained that the organizational charts were reviewed by appropriate Atlassian management and updated semi-annually, as appropriate.	No deviation noted.
	Inspected the organizational charts and ascertained that the appropriate Atlassian management reviewed and updated semi-annually, as appropriate.	No deviation noted.

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

CC 1.0 Common Criteria Related to Control Environment

CC 1.4 The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Policies are posted and available online, assigned a policy owner, and reviewed at least annually by the designated policy owner or their delegate.	Inquired of the control owner and ascertained that policies were posted and available online, assigned a policy owner, and reviewed at least annually by the designated policy owner.	No deviation noted.
	Inspected the policies and ascertained that the policies were posted and available online, assigned a policy owner, and reviewed at least annually by the designated policy owner.	No deviation noted.
At least annually, the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) have annually reviewed committee charters and corporate governance which define their roles, responsibilities, meeting frequency, participants, member qualifications, and discussion topics.	Inquired of the control owner and ascertained that the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) reviewed committee charters and corporate governance which defined their roles, responsibilities, meeting frequency, participants, member qualifications on an annual basis.	No deviation noted.
	Inspected the current year's Board of Directors and subcommittee annual meeting minutes, and ascertained that committee charters and corporate governance, which defined their roles, responsibilities, meeting frequency, participants, and member qualifications, were discussed.	No deviation noted.
The process of identifying and reviewing Board of Director candidates is defined In Nominating and Governance Committee charter.	Inquired of the control owner and ascertained the process of identifying and reviewing Board of Director candidates was defined in Nominating and Governance Committee charter.	No deviation noted.
	Inspected the Nominating and Governance committee charter, and ascertained that the process of identifying and reviewing Board of Director candidates was defined.	No deviation noted.
Vendor agreements, including any security, availability and	Inquired of the control owner and ascertained that vendor agreements, including any security, availability, and	No deviation noted.

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

CC 1.0 Common Criteria Related to Control Environment

CC 1.4 The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
confidentiality commitments, are reviewed during the procurement process.	confidentiality commitments, were reviewed during the procurement process.	
	Inspected a sample of new vendors' third-party contracts and ascertained that the contracts included security, availability, and confidentiality commitments, and the contracts were executed between the third-party and Atlassian during the procurement process.	No deviation noted.
For every external offer that goes out, the manager or manager's manager will approve the offer or the HRIS team will approve on behalf of the manager if there is a peer or higher that has approved outside the system. The exception to this process is contractors, interns and graduates. • For contractors, who are	Inquired of the control owner and ascertained that for every external offer that goes out, the manager would approve the offer or the HRIS team would approve on behalf of the manager if there was a peer or higher that had approved outside the system. Further inquired and ascertained that for contractors, who were hired outside of the standard hiring process, there was a confirmation of screening step in the onboarding process within Service Desk. A recruiting manager would approve the offer letters for Interns and Grads because of the bulk nature and timing of these hires.	No deviation noted.

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

CC 1.0 Common Criteria Related to Control Environment

CC 1.4 The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
hired outside of the standard hiring process, there is a confirmation of screening step in the onboarding process within Service Desk. • A Recruiting Manager will approve the offer letters for Interns and Grads because of the bulk nature and timing of these hires.	Inspected a sample of job offers of new hires, interns, graduates, and contractors, and ascertained that job offers were reviewed and approved by a manager or confirmation of screening step in the onboarding process within Service Desk prior to hiring.	No deviation noted.
Background checks are performed prior to their start date. Results are reviewed against a results matrix and escalated to Legal and Head of HR Operations, if needed.	Inquired of the control owner and ascertained that background checks were performed prior to a new hire's start date. Results were reviewed against a results matrix and escalated to Legal and Head of HR Operations, if needed.	No deviation noted.
	Inspected the background check results for a sample of new employees and contractors, and ascertained that background checks were performed prior to their start date. Further ascertained that results were reviewed against a results matrix and escalated to Legal and Head of HR Operations, if needed.	No deviation noted.
User awareness training is performed at least annually as part of the Atlassian Security Awareness program.	Inquired of the control owner and ascertained that user awareness training for malware risks was part of the security awareness program at Atlassian and performed at least on an annual basis.	No deviation noted.
	Inspected the user awareness training e-mail and security homepage, and ascertained that security training, including passwords, phishing, and travel security, were updated, posted,	No deviation noted.

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

CC 1.0 Common Criteria Related to Control Environment

CC 1.4 The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	and available for all employees as part of the security awareness program at Atlassian.	
Performance appraisals are performed at least annually.	Inquired of the control owner and ascertained that performance appraisals were conducted at least annually.	No deviation noted.
	Inspected the performance appraisal results for a sample of employees and ascertained that performance appraisals were conducted at least annually.	The performance appraisals have not been performed during the audit period. The annual performance appraisals are performed between June and July annually. The last performance appraisals were performed in July 2019 and the next assessment is expected to be completed in July 2020.
Training is provided to employees to support their continued development and growth.	Inquired of the control owner and ascertained that employees are provided with the necessary training and support to continue to learn and grow.	No deviation noted.
	Inspected the training homepage and ascertained that training and support was provided to employees through the training homepage and employees can continue to learn and grow.	No deviation noted.

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

CC 1.0 Common Criteria Related to Control Environment

CC 1.5 The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Policies are posted and available online, assigned a policy owner, and reviewed at least annually by the designated policy owner or their delegate.	Inquired of the control owner and ascertained that policies were posted and available online, assigned a policy owner, and reviewed at least annually by the designated policy owner.	No deviation noted.
	Inspected the policies and ascertained that the policies were posted and available online, assigned a policy owner, and reviewed at least annually by the designated policy owner.	No deviation noted.
At least annually, the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) have annually reviewed committee charters and corporate governance which define their roles, responsibilities, meeting frequency, participants, member qualifications, and discussion topics.	Inquired of the control owner and ascertained that the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) reviewed committee charters and corporate governance which defined their roles, responsibilities, meeting frequency, participants, member qualifications on an annual basis.	No deviation noted.
	Inspected the current year's Board of Directors and subcommittee annual meeting minutes, and ascertained that committee charters and corporate governance, which defined their roles, responsibilities, meeting frequency, participants, and member qualifications, were discussed.	No deviation noted.
New employees are assigned a 90 day onboarding plan.	Inquired of the control owner and ascertained that new employees were assigned a 90-day onboarding plan.	No deviation noted.
	Inspected the 90-day onboarding plan for a sample of new employees and ascertained that employees were assigned a 90-day onboarding plan.	No deviation noted.
Employees and contractors are required to sign CIIAs as part of the onboarding process.	Inquired of the control owner and ascertained that employees and contractors were required to sign CIIAs as part of the onboarding process.	No deviation noted.

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

CC 1.0 Common Criteria Related to Control Environment

CC 1.5 The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	Inspected the signed CIIAs for a sample of new employees and contractors, and ascertained that employees and contractors were required to sign CIIAs as part of the onboarding process.	No deviation noted.
Employees and contractors acknowledge the Code of Conduct annually.	Inquired of the control owner and ascertained that employees as well as contractors, acknowledged the Code of Conduct annually.	No deviation noted.
	Inspected the code of conduct acknowledgement for a sample of active employees and contractors, and ascertained that employees as well as contractors acknowledged the Code of Conduct annually.	No deviation noted.
Performance appraisals are performed at least annually.	Inquired of the control owner and ascertained that performance appraisals were conducted at least annually.	No deviation noted.
	Inspected the performance appraisal results for a sample of employees and ascertained that performance appraisals were conducted at least annually.	The performance appraisals have not been performed during the audit period. The annual performance appraisals are performed between June and July annually. The last performance appraisals were performed in July 2019 and the next assessment is expected to be completed in July 2020.

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

CC 1.0 Common Criteria Related to Control Environment

CC 1.5 The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Training is provided to employees to support their continued development and growth.	Inquired of the control owner and ascertained that employees are provided with the necessary training and support to continue to learn and grow.	No deviation noted.
	Inspected the training homepage and ascertained that training and support was provided to employees through the training homepage and employees can continue to learn and grow.	No deviation noted.

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

CC 2.0 Common Criteria Related to Communication and Information

CC 2.1 The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
At least annually, the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) have annually reviewed committee charters and corporate governance which define their roles, responsibilities, meeting frequency, participants, member qualifications, and discussion topics.	Inquired of the control owner and ascertained that the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) reviewed committee charters and corporate governance which defined their roles, responsibilities, meeting frequency, participants, member qualifications on an annual basis.	No deviation noted.
	Inspected the current year's Board of Directors and subcommittee annual meeting minutes, and ascertained that committee charters and corporate governance, which defined their roles, responsibilities, meeting frequency, participants, and member qualifications, were discussed.	No deviation noted.
Audit Committee Charter defines roles, responsibilities, and key activities of the audit committee.	Inquired of the control owner and ascertained that Audit Committee Charter defines roles, responsibilities, and key activities of the audit committee.	No deviation noted.
	Inspected the Audit Committee Charter in the Atlassian's website and ascertained that roles, responsibilities, and key activities of the audit committee were defined.	No deviation noted.
Audit Committee meeting calendar and general meeting agenda are developed.	Inquired of the control owner and ascertained that Audit Committee meeting calendar and general meeting agendas were developed.	No deviation noted.
	Inspected the Audit Committee latest notice for the annual general meeting and ascertained that Audit Committee meeting calendar and general meeting agendas were developed.	No deviation noted.
Qualifications for the Audit Committee's "Financial Expert"	Inquired of the control owner and ascertained that the Audit Committee Charter defined the qualifications for the Audit Committee's "Financial Expert".	No deviation noted.

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

CC 2.0 Common Criteria Related to Communication and Information

CC 2.1 The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
have been defined in the audit committee charter.	Inspected the Audit Committee Charter in the Atlassian's website and ascertained that qualifications for the "Financial Expert" was defined.	No deviation noted.
Financial statement risk assessment performed by Internal Audit and reviewed by Controller.	Inquired of the control owner and ascertained that on an annual basis, the Controller reviews the financial statement risk assessments based on knowledge of the Company and against the assumptions used in the prior year.	No deviation noted.
	Inspected that most recent financial statement risk assessment and ascertained that the financial statement risk was reviewed by the Controller on an annual basis.	The annual financial statement risk assessment has not been completed during the audit period (November 1, 2019 to March 31, 2020). The annual financial statement risk assessment is performed every October. The last financial statement risk assessment was completed on October 18, 2019.

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

CC 2.0 Common Criteria Related to Communication and Information

CC 2.1 The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
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.	Inquired of the control owner and ascertained that the fraud risk assessment was performed on an annual basis by the Head of Risk and Compliance. Further ascertained that this included a survey of employees susceptible to fraud and evaluation of external risks. The results were evaluated by the Head of Risk and Compliance and included in the enterprise risk assessment communicated to the board and executive level managers annually.	No deviation noted.
	Inspected the most recent enterprise risk assessment and ascertained that the enterprise risk assessment included fraud risk assessment, which was performed and evaluated annually by the Head of Risk and Compliance.	No deviation noted.
	Inspected the most recent fraud risk assessment and ascertained that the assessment was performed and evaluated annually by the Head of Risk and Compliance. Further ascertained that a cross-functional survey of employees in areas susceptible to fraud was conducted and combined with an evaluation of external risks, and the results were included with the enterprise risk assessment. Additionally, ascertained that the results were communicated to the board and executive level managers as part of the annual meeting held.	The annual fraud risk assessment has not been completed during the audit period (November 1, 2019 to March 31, 2020). However, the Risk and Compliance Team performs the fraud risk assessment as part of the periodic enterprise risk assessment. The annual fraud risk assessment was initiated in December 2019 and

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

CC 2.0 Common Criteria Related to Communication and Information

CC 2.1 The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
		will be completed in June 2020. The last fraud risk assessment was performed and completed in June 2019.
Internal audits are performed, results are communicated, and corrective actions are monitored.	Inquired of the Internal Audit and ascertained that internal audits were performed relating to SOX, ISO, SOC, and other operational audits. Further ascertained that results were communicated, and corrective actions were monitored.	No deviation noted.
	Inspected the GRC tool and Jira ticket and ascertained that internal audits were performed relating to SOX, ISO, SOC, and other operational audits. Further ascertained that results were communicated, and corrective actions were monitored.	No deviation noted.
The Micros platform will not allow code artefacts to deploy or run on the platform unless they have been peer reviewed and have passed green build testing.	Inquired of the control owner and ascertained that changes were documented through pull requests, and peer review and passed green build testing was required prior to merging the code to the master branch.	No deviation noted.
	Inspected the Bitbucket configuration and ascertained that changes were documented through pull requests, and that the Bitbucket repositories would not allow changes to deploy or run on the platform unless they have been peer reviewed and have passed green build testing.	No deviation noted.
	Inspected a sample of merged pull requests and ascertained that documented peer review and green build testing was required prior to merging the code to master branch.	No deviation noted.

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

CC 2.0 Common Criteria Related to Communication and Information

CC 2.1 The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Micros will only pull deployment artefacts from the restricted namespace. Only deployment-bamboo has the credentials to push to the restricted namespace.	Inquired of the control owner and ascertained that artefacts with peer review and passed green build testing were deployed from a restricted namespace by deployment-bamboo bot account.	No deviation noted.
	Inspected the list of accounts with ability to commit changes to Docker and ascertained that only deployment-bamboo was assigned to push changes to Docker.	No deviation noted.
	Attempted to push a change to the restricted Docker namespace using an end user account and ascertained that the deployed change was denied.	No deviation noted.
Bitbucket does not allow a pull request to be approved by the same user who requests it.	Inquired of the control owner and ascertained that Bitbucket does not allow a pull requests to be approved by the same user who requests it.	No deviation noted.
	Attempted a creation of pull request and ascertained that Bitbucket did not allow a pull request to be approved by the same user who requested it.	No deviation noted.
	Inspected a sample of merged pull requests and ascertained that the peer reviewer requester was not the same as the approver.	No deviation noted.
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.	Inquired of the control owner and ascertained that Bamboo would not allow code to be deployed unless it has passed green build testing.	No deviation noted.
	Attempted to deploy a red build code and ascertained that it did not allow the code to be deployed unless it has passed green build testing.	No deviation noted.
	Attempted to deploy a green build code and ascertained that Bamboo allowed the code to be deployed.	No deviation noted

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

CC 2.0 Common Criteria Related to Communication and Information

CC 2.1 The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
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 were not enforced, the code is rejected.	Inquired of the control owner and ascertained that 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.	No deviation noted.
	Inspected the API configuration in Deployment bamboo and ascertained that a check was performed to validate that the SOX settings on Bitbucket were 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.	No deviation noted.
	Attempted to deploy a change that was not compliant and ascertained that the code was rejected for deployment upon the validation check in Deployment Bamboo.	No deviation noted.
	Attempted to deploy a change that was compliant and ascertained that the code was successfully deployed upon the validation check in Deployment Bamboo.	No deviation noted.

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

CC 2.0 Common Criteria Related to Communication and Information

CC 2.1 The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Privileged access to Deployment Bamboo is restricted to the members of the Build Engineering team.	Inquired of the control owner and ascertained that privileged access to Deployment Bamboo was restricted to the members of the Build Engineering team.	No deviation noted.
	Inspected the list of users with privileged access to Deployment Bamboo and ascertained that access was restricted to the members of the Build Engineering team.	No deviation noted.
On a semi-annual basis, the Build Engineering Development Team Lead performs a review of privileged user access for Deployment bamboo.	Inquired of the control owner and ascertained that the Build Engineering Development Team Lead performed a review of privileged user access for Deployment bamboo semi-annually.	No deviation noted.
	Inspected a sampled user access review report and ascertained that the Build Engineering Development Team Lead performed a review of privileged user access for Deployment bamboo semi-annually.	No deviation noted.
A Jira ticket is automatically generated if a change to the enforcement of peer review/pull requests occurs.	Inquired of the control owner and ascertained that a Jira ticket was automatically generated if a change to the enforcement of peer review or pull request occurs.	No deviation noted.
	Inspected the configuration and ascertained that a Jira ticket was automatically generated if a change to the enforcement of peer review or pull request occurs.	No deviation noted.

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

CC 2.0 Common Criteria Related to Communication and Information

CC 2.2 The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Employees and contractors are required to sign CIIAs as part of the onboarding process.	Inquired of the control owner and ascertained that employees and contractors were required to sign CIIAs as part of the onboarding process.	No deviation noted.
	Inspected the signed CIIAs for a sample of new employees and contractors, and ascertained that employees and contractors were required to sign CIIAs as part of the onboarding process.	No deviation noted.
New employees are assigned a 90 day onboarding plan.	Inquired of the control owner and ascertained that new employees were assigned a 90-day onboarding plan.	No deviation noted.
	Inspected the 90-day onboarding plan for a sample of new employees and ascertained that employees were assigned a 90-day onboarding plan.	No deviation noted.
Employees and contractors acknowledge the Code of Conduct annually.	Inquired of the control owner and ascertained that employees as well as contractors, acknowledged the Code of Conduct annually.	No deviation noted.
	Inspected the code of conduct acknowledgement for a sample of active employees and contractors, and ascertained that employees as well as contractors acknowledged the Code of Conduct annually.	No deviation noted.
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.	Inquired of the control owner and ascertained that a weekly review was performed to determine that the CIIA (Confidential Information and Inventions Assignment) and that background checks were completed prior to their start date.	No deviation noted.

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

CC 2.0 Common Criteria Related to Communication and Information

CC 2.2 The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	Inspected the reviews for a sample of week and ascertained that a weekly review was performed to determine that new employees complete the CIIA (Confidential Information and Inventions Assignment) and background checks were completed prior to their start date.	No deviation noted.
User awareness training is performed at least annually as part of the Atlassian Security Awareness program.	Inquired of the control owner and ascertained that user awareness training for malware risks was part of the security awareness program at Atlassian and performed at least on an annual basis.	No deviation noted.
	Inspected the user awareness training e-mail and security homepage, and ascertained that security training, including passwords, phishing, and travel security, were updated, posted, and available for all employees as part of the security awareness program at Atlassian.	No deviation noted.
At least annually, the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) have annually reviewed committee charters and corporate governance which define their roles, responsibilities, meeting frequency, participants, member qualifications, and discussion topics.	Inquired of the control owner and ascertained that the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) reviewed committee charters and corporate governance which defined their roles, responsibilities, meeting frequency, participants, member qualifications on an annual basis.	No deviation noted.
	Inspected the current year's Board of Directors and subcommittee annual meeting minutes, and ascertained that committee charters and corporate governance, which defined their roles, responsibilities, meeting frequency, participants, and member qualifications, were discussed.	No deviation noted.

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

CC 2.0 Common Criteria Related to Communication and Information

CC 2.2 The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Atlassian has established a Whistleblower hotline that is accessible to both external individuals and employees within the Company.	Inquired of the control owner and ascertained the Company had established a Whistleblower hotline that was accessible to both external individuals and employees within the Company.	No deviation noted.
	Inspected that Whistleblower hotline configuration and ascertained that the hotline was operating for external individuals and employees within the Company. Further inspected the notification alert and ascertained that all claims would notify to the General Counsel, Associate General Counsel, the Head of Internal Audit, and Audit Committee Chair.	No deviation noted.
Users (either internal or external) may report bugs, defects, or availability, security, and confidentiality issues via https://getsupport.atlassian.com, social media, general website forms, emails, https://trust.atlassian.com, and the public bug site.	Inquired of the control owner and ascertained that customers and internal users contacted Atlassian to report issues on bugs, defects, availability, security, and confidentiality via https://getsupport.atlassian.com, social media, general website forms, emails, https://trust.atlassian.com, and the public bug site.	No deviation noted.
	Inspected the channels of reporting for issues and ascertained that customers and internal users can contact Atlassian to report issues on bugs, defects, availability, security, and confidentiality via https://getsupport.atlassian.com, social media, general website forms, emails, https://trust.atlassian.com, and the public bug site.	No deviation noted.
	Inspected a sample of issues reported by either internal or external users, and ascertained that issues were followed up and resolved per incident management process.	No deviation noted.
An organizational wide incident management process is in place, with the SRE team responsible for	Inquired of the control owner and ascertained that incident management process was in place, the Site Reliability ("SRE") team was responsible for incidents and problems for Atlassian	No deviation noted.

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

CC 2.0 Common Criteria Related to Communication and Information

CC 2.2 The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
incidents and problems for Atlassian services and platforms. Incident management process must meet the Atlassian Incident Management Standard.	services and platforms, and that incident management process met the Atlassian Incident Management Standard. Further ascertained that for incidents with severity 0 and 1, a post incident review ("PIR") and root cause analysis were performed. Further ascertained that for incidents with security level 2 and 3, a post incident review express ("PIR-X") was performed.	
	Inspected a sample of incidents and issues from the incident reporting and tracking system, and ascertained that incidents and issues were monitored and resolved timely. If Jira ticket corresponded to severity level 0 and 1, ascertained that post incident review ("PIR") and root cause analysis were performed. If a Jira ticket corresponded to severity level 2 and 3, ascertained that post incident review express ("PIR-X") was performed.	No deviation noted.
A description of the system delineating the boundaries and describing relevant components is documented on the Atlassian intranet and the customer-facing website.	Inquired of the control owner and ascertained that the description of the system delineating the boundaries and describing relevant components was documented on the Atlassian intranet and the customer-facing website.	No deviation noted.
	Inspected the Atlassian intranet and the customer-facing website, and ascertained that the description of the Statuspage system delineating the boundaries and describing relevant components were documented and posted.	No deviation noted.
Atlassian communicates its commitment to security as a top priority for its customers via Atlassian Trust Security page.	Inquired of the control owner and ascertained that Atlassian communicated its commitment to security as a top priority for its customers on the Atlassian Trust Security page.	No deviation noted.
	Inspected the Atlassian Trust Security Page and ascertained that Atlassian communicated its commitment to security as a top priority for its customers via Atlassian Trust Security page.	No deviation noted.

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

CC 2.0 Common Criteria Related to Communication and Information

CC 2.2 The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Atlassian communicates changes to confidentiality commitments to its customers, vendors and internal users through the Atlassian website, when applicable.	Inquired of the control owner and ascertained that Atlassian communicated changes to confidentiality commitments to its customers, vendors, and internal users through the Atlassian website, when applicable.	No deviation noted.
	Inspected the Atlassian's website and ascertained that communication on changes to confidentiality commitments to its customers, vendors, and internal users were posted when applicable.	No deviation noted.
Significant changes made to the system are communicated to internal users and customers.	Inquired of the control owner and ascertained that significant changes made to the systems were communicated to internal and external users.	No deviation noted.
	Inspected the customer-facing website and intranet, and ascertained that significant changes made to the Statuspage system were communicated to internal and external users.	No deviation noted.
Monitoring tools are in place to track and notify on the availability of Statuspage systems and services.	Inquired of the control owner and ascertained that Statuspage has monitoring tools in place to track and notify on the availability of Statuspage systems and services.	No deviation noted.
	Inspected the configuration of the monitoring tools in place and ascertained that monitoring tools were in place to monitor system availability of Statuspage systems and services.	No deviation noted.
	Inspected the configuration of the alert settings and ascertained that notifications were communicated to the appropriate Statuspage and Micros group.	No deviation noted.
	Inspected the resolution for a sample of HOT tickets created and ascertained that corrective actions were followed up and timely resolved.	No deviation noted.

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

CC 2.0 Common Criteria Related to Communication and Information

CC 2.3 The entity communicates with external parties regarding matters affecting the functioning of internal control.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
At least annually, the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) have annually reviewed committee charters and corporate governance which define their roles, responsibilities, meeting frequency, participants, member qualifications, and discussion topics.	Inquired of the control owner and ascertained that the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) reviewed committee charters and corporate governance which defined their roles, responsibilities, meeting frequency, participants, member qualifications on an annual basis.	No deviation noted.
	Inspected the current year's Board of Directors and subcommittee annual meeting minutes, and ascertained that committee charters and corporate governance, which defined their roles, responsibilities, meeting frequency, participants, and member qualifications, were discussed.	No deviation noted.
Audit Committee Charter defines roles, responsibilities, and key activities of the audit committee.	Inquired of the control owner and ascertained that Audit Committee Charter defines roles, responsibilities, and key activities of the audit committee.	No deviation noted.
	Inspected the Audit Committee Charter in the Atlassian's website and ascertained that roles, responsibilities, and key activities of the audit committee were defined.	No deviation noted.
Audit Committee Meeting calendar and general meeting agenda are developed.	Inquired of the control owner and ascertained that Audit Committee meeting calendar and general meeting agendas were developed.	No deviation noted.
	Inspected the Audit Committee latest notice for the annual general meeting and ascertained that Audit Committee meeting calendar and general meeting agendas were developed.	No deviation noted.
Qualifications for the Audit Committee's "Financial Expert"	Inquired of the control owner and ascertained that the Audit Committee Charter defined the qualifications for the Audit Committee's "Financial Expert".	No deviation noted.

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

CC 2.0 Common Criteria Related to Communication and Information

CC 2.3 The entity communicates with external parties regarding matters affecting the functioning of internal control.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
have been defined in the audit committee charter.	Inspected the Audit Committee Charter in the Atlassian's website and ascertained that qualifications for the "Financial Expert" was defined.	No deviation noted.
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.	Inquired of the control owner and ascertained that the fraud risk assessment was performed on an annual basis by the Head of Risk and Compliance. Further ascertained that this included a survey of employees susceptible to fraud and evaluation of external risks. The results were evaluated by the Head of Risk and Compliance and included in the enterprise risk assessment communicated to the board and executive level managers annually.	No deviation noted.
	Inspected the most recent Enterprise Risk Management ("ERM") assessment and ascertained that Atlassian had defined an ERM process, and the enterprise risk assessment was performed on an annual basis, which includes key product stakeholders. Further ascertained that a fraud risk assessment was performed as part of the ERM assessment. Additionally, a monthly meeting was held to discuss updates to the enterprise and fraud risk assessment and results.	No deviation noted.
	Inspected the most recent fraud and enterprise risk assessment and ascertained that the assessment was performed and evaluated annually by the Head of Risk and Compliance. Further ascertained that a cross-functional survey of employees in areas susceptible to fraud was conducted and combined with an evaluation of external risks, and the results were included with the enterprise risk assessment. Additionally, ascertained that the results were communicated to the board and executive level managers as part of the annual meeting held.	The annual fraud risk assessment has not been completed during the audit period (November 1, 2019 to March 31, 2020). However, the Risk and Compliance Team performs fraud risk assessment as part of

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

CC 2.0 Common Criteria Related to Communication and Information

CC 2.3 The entity communicates with external parties regarding matters affecting the functioning of internal control.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
		the periodic enterprise risk assessment.
Atlassian has established a Whistleblower hotline that is accessible to both external individuals and employees within the Company.	Inquired of the control owner and ascertained the Company had established a Whistleblower hotline that was accessible to both external individuals and employees within the Company.	No deviation noted.
	Inspected that Whistleblower hotline configuration and ascertained that the hotline was operating for external individuals and employees within the Company. Further inspected the notification alert and ascertained that all claims would notify to the General Counsel, Associate General Counsel, the Head of Internal Audit, and Audit Committee Chair.	No deviation noted.
Vendor agreements, including any security, availability and confidentiality commitments, are reviewed during the procurement process.	Inquired of the control owner and ascertained that vendor agreements, including any security, availability, and confidentiality commitments, were reviewed during the procurement process.	No deviation noted.
	Inspected a sample of new vendors' third-party contracts and ascertained that the contracts included security, availability, and confidentiality commitments, and the contracts were executed between the third-party and Atlassian during the procurement process.	No deviation noted.
Atlassian reviews the SOC reports of the vendors on an annual basis.	Inquired of the control owner and ascertained that Atlassian reviewed the SOC reports of the vendors ("subservice organizations") on an annual basis.	No deviation noted.
	Inspected the Jira ticket for the review of the SOC 2 or equivalent attestation reports and ascertained that leadership reviewed the reports annually. Reviews included an assessment of complementary user entity controls, subservice organizations, and mapping of the controls to key risks. If there	No deviation noted.

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

CC 2.0 Common Criteria Related to Communication and Information

CC 2.3 The entity communicates with external parties regarding matters affecting the functioning of internal control.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	were exceptions, Atlassian reviewed the severity and impact of the exceptions, and if needed, followed-up with the individual vendor.	
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.	Inquired of the control owner and ascertained that customer terms of service were standardized and approved by legal. The terms of service communicate the security, availability, and confidentiality commitments to the customer and any changes were communicated.	No deviation noted.
	Inspected the Atlassian Customer Agreement and ascertained that security, availability, and confidentiality commitments were communicated to the customer prior to purchase of products or creation of user accounts, and any changes were communicated.	No deviation noted.
	Inspected the contract agreement between Atlassian (Legal) and Channel Partners and ascertained that Channel Partners were responsible for ensuring each end user had entered into a customer agreement between the Channel Partners and the end customer, and that the Channel Partners were responsible for all liabilities and expenses to end customers.	No deviation noted.
Users (either internal or external) may report bugs, defects, or availability, security, and confidentiality issues via https://getsupport.atlassian.com, social media, general website	Inquired of the control owner and ascertained that customers and internal users contacted Atlassian to report issues on bugs, defects, availability, security, and confidentiality via https://getsupport.atlassian.com, social media, general website forms, emails, https://trust.atlassian.com, and the public bug site.	No deviation noted.

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

CC 2.0 Common Criteria Related to Communication and Information

CC 2.3 The entity communicates with external parties regarding matters affecting the functioning of internal control.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
forms, emails, https://trust.atlassian.com, and the public bug site.	Inspected the channels of reporting for issues and ascertained that customers and internal users can contact Atlassian to report issues on bugs, defects, availability, security, and confidentiality via https://getsupport.atlassian.com, social media, general website forms, emails, https://trust.atlassian.com, and the public bug site.	No deviation noted.
	Inspected a sample of issues reported by either internal or external users, and ascertained that issues were followed up and resolved per incident management process.	No deviation noted.
Customer responsibilities are described on the Atlassian customer-facing website.	Inquired of the control owner and ascertained that customer responsibilities were described on the Atlassian customer-facing website.	No deviation noted.
	Inspected the Atlassian's customer-facing website and ascertained customer responsibilities were described and posted.	No deviation noted.
A description of the system delineating the boundaries and describing relevant components is documented on the Atlassian intranet and the customer-facing website.	Inquired of the control owner and ascertained that the description of the system delineating the boundaries and describing relevant components was documented on the Atlassian intranet and the customer-facing website.	No deviation noted.
	Inspected the Atlassian intranet and the customer-facing website, and ascertained that the description of the Statuspage system delineating the boundaries and describing relevant components were documented and posted.	No deviation noted.
Atlassian communicates its commitment to security as a top	Inquired of the control owner and ascertained that Atlassian communicated its commitment to security as a top priority for its customers on the Atlassian Trust Security page.	No deviation noted.

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

CC 2.0 Common Criteria Related to Communication and Information

CC 2.3 The entity communicates with external parties regarding matters affecting the functioning of internal control.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
priority for its customers via Atlassian Trust Security page.	Inspected the Atlassian Trust Security Page and ascertained that Atlassian communicated its commitment to security as a top priority for its customers via Atlassian Trust Security page.	No deviation noted.
Atlassian communicates changes to confidentiality commitments to its customers, vendors and internal users through the Atlassian website, when applicable.	Inquired of the control owner and ascertained that Atlassian communicated changes to confidentiality commitments to its customers, vendors, and internal users through the Atlassian website, when applicable.	No deviation noted.
	Inspected the Atlassian's website and ascertained that communication on changes to confidentiality commitments to its customers, vendors, and internal users were posted when applicable.	No deviation noted.
Significant changes made to the system are communicated to internal users and customers.	Inquired of the control owner and ascertained that significant changes made to the systems were communicated to internal and external users.	No deviation noted.
	Inspected the customer-facing website and intranet, and ascertained that significant changes made to the Statuspage system were communicated to internal and external users.	No deviation noted.
Availability is published so that Customers may check the status/uptime of Statuspage.	Inquired of the control owner and ascertained that availability was published in the customer-facing website so that customers could check the status and uptime of Statuspage.	No deviation noted.
	Inspected the customer-facing website and ascertained that availability was published real-time, and the status and uptime metrics of Statuspage were communicated to customers.	No deviation noted.
Monitoring tools are in place to track and notify on the	Inquired of the control owner and ascertained that Statuspage has monitoring tools in place to track and notify on the availability of Statuspage systems and services.	No deviation noted.

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

CC 2.0 Common Criteria Related to Communication and Information

CC 2.3 The entity communicates with external parties regarding matters affecting the functioning of internal control.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
availability of Statuspage systems and services.	Inspected the configuration of the monitoring tools in place and ascertained that monitoring tools were in place to monitor system availability of Statuspage systems and services.	No deviation noted.
	Inspected the configuration of the alert settings and ascertained that notifications were communicated to the appropriate Statuspage and Micros group.	No deviation noted.
	Inspected the resolution for a sample of HOT tickets created and ascertained that corrective actions were followed up and timely resolved.	No deviation noted.
Employees and contractors acknowledge the Code of Conduct annually.	Inquired of the control owner and ascertained that employees as well as contractors, acknowledged the Code of Conduct annually.	No deviation noted.
	Inspected the code of conduct acknowledgement for a sample of active employees and contractors, and ascertained that employees as well as contractors acknowledged the Code of Conduct annually.	No deviation noted.

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

CC 3.0 Common Criteria Related to Risk Assessment

CC3.1 The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Atlassian has defined an ERM process and conducts an enterprise risk assessment on an annual basis, which includes key product stakeholders.	Inquired of the control owner and ascertained that Atlassian had defined a risk management process, and conducted an enterprise risk assessment on an annual basis, inclusive of key product stakeholders.	No deviation noted.
	Inspected the ERM assessment and ascertained that Atlassian had defined an ERM process, and the enterprise risk assessment was performed on an annual basis, which includes key product stakeholders. Additionally, a monthly meeting was held to discuss updates to the enterprise risk assessment and results.	No deviation noted.
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.	Inquired of the control owner and ascertained that the Atlassian Risk and Compliance team evaluated the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Atlassian maintained a risk and controls matrix within their GRC tool.	No deviation noted.
	Inspected the GRC Tool used by Atlassian and ascertained that the Atlassian Risk and Compliance team evaluated the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Further ascertained that Atlassian maintained a risk and controls matrix within their GRC tool.	No deviation noted.
Internal audits are performed, results are communicated, and corrective actions are monitored.	Inquired of the Internal Audit and ascertained that internal audits were performed relating to SOX, ISO, SOC, and other operational audits. Further ascertained that results were communicated, and corrective actions were monitored.	No deviation noted.
	Inspected the GRC tool and Jira ticket and ascertained that internal audits were performed relating to SOX, ISO, SOC, and	No deviation noted.

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

CC 3.0 Common Criteria Related to Risk Assessment

CC3.1 The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	other operational audits. Further ascertained that results were communicated, and corrective actions were monitored.	
At least annually, the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) have annually reviewed committee charters and corporate governance which define their roles, responsibilities, meeting frequency, participants, member qualifications, and discussion topics.	Inquired of the control owner and ascertained that the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) reviewed committee charters and corporate governance which defined their roles, responsibilities, meeting frequency, participants, member qualifications on an annual basis.	No deviation noted.
	Inspected the current year's Board of Directors and subcommittee annual meeting minutes, and ascertained that committee charters and corporate governance, which defined their roles, responsibilities, meeting frequency, participants, and member qualifications, were discussed.	No deviation noted.
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	Inquired of the control owner and ascertained that the fraud risk assessment was performed on an annual basis by the Head of Risk and Compliance. Further ascertained that this included a survey of employees susceptible to fraud and evaluation of external risks. The results were evaluated by the Head of Risk and Compliance and included in the enterprise risk assessment communicated to the board and executive level managers annually.	No deviation noted.
	Inspected the most recent enterprise risk assessment and ascertained that the enterprise risk assessment included fraud risk assessment, which was performed and evaluated annually by the Head of Risk and Compliance.	No deviation noted.

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

CC 3.0 Common Criteria Related to Risk Assessment

CC3.1 The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
communicated to the board and executive level managers annually.	Inspected the most recent fraud and enterprise risk assessment and ascertained that the assessment was performed and evaluated annually by the Head of Risk and Compliance. Further ascertained that a cross-functional survey of employees in areas susceptible to fraud was conducted and combined with an evaluation of external risks, and the results were included with the enterprise risk assessment. Additionally, ascertained that the results were communicated to the board and executive level managers as part of the annual meeting held.	The annual fraud risk assessment has not been completed during the audit period (November 1, 2019 to March 31, 2020). However, the Risk and Compliance Team performs fraud risk assessment as part of the periodic enterprise risk assessment. The annual fraud risk assessment was initiated in December 2019 and will be completed in June 2020. The last fraud risk assessment was performed and completed in June 2019.
Financial statement risk assessment performed by Internal Audit and reviewed by Controller.	Inquired of the control owner and ascertained that on an annual basis, the Controller reviews the financial statement risk assessments based on knowledge of the Company and against the assumptions used in the prior year.	No deviation noted.

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

CC 3.0 Common Criteria Related to Risk Assessment

CC3.1 The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	Inspected that most recent financial statement risk assessment and ascertained that the financial statement risk was reviewed by the Controller on an annual basis.	The annual financial statement risk assessment has not been completed during the audit period (November 1, 2019 to March 31, 2020). The annual financial statement risk assessment is performed every October. The last financial statement risk assessment was completed on October 18, 2019.
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	Inquired of the control owner and ascertained a standard disclosure checklist was completed by a member of Technical Accounting to identify areas for disclosure annually. Additionally, the Head of Technical Accounting and Financial Reporting reviewed the electronic copy of the checklist for completeness and accuracy of responses provided with evidences review and approval documented via the Jira Service Desk.	No deviation noted.

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

CC 3.0 Common Criteria Related to Risk Assessment

CC3.1 The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
completeness and accuracy of responses provided and evidences review and approval via Jira Service Desk.	Inspected the standard disclosure checklist and ascertained that the checklist was completed by a member of the Technical Accounting Team at least annually, and areas of disclosures were identified. Further ascertained that the checklist was reviewed by the Head of Technical Accounting and Financial Reporting for completeness and accuracy of responses provided per inspection of the associated Jira Service Desk ticket.	No deviation noted.
The Head of Technical Accounting and Financial Reporting 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.	Inquired of the control owner and ascertained the Head of Technical Accounting and Financial Reporting reviewed the financials and footnote disclosures prepared by the member of Technical Accounting for reasonableness, internal consistency, and confirmed prior period balances of the final financial statements. A copy of the reviewed statements was then attached to an email to the CFO to evidence completion of review.	No deviation noted.
	Inspected the financials and footnote disclosures review and ascertained that the Head of Technical Accounting and Financial Reporting reviewed the financials and footnote disclosures prepared by a member of Technical Accounting for reasonableness and internal consistency, and confirmed prior period balances in the financial statements.	No deviation noted.
The signature authority matrix is maintained by Legal which establishes the signature authority for expenditures, contracts, capital acquisitions and write offs. Separately, the	Inquired of the control owner and ascertained the Spend Authority Limits (Signature Authority Matrix) was maintained by Legal, which establishes the signature authority for expenditures, contracts, capital acquisitions, and write offs. The Corporate Controller separately establishes the cash disbursement.	No deviation noted.

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

CC 3.0 Common Criteria Related to Risk Assessment

CC3.1 The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Corporate Controller established the cash disbursement.	Inspected the signature authority matrix and ascertained that legal approved and maintained the signature authority for expenditures, contracts, capital acquisitions, and write offs. Further ascertained that expenditure limits were reviewed annually during the Board of Directors meeting with the corporate controller establishing the cash disbursement.	No deviation noted.

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

CC 3.0 Common Criteria Related to Risk Assessment

CC 3.2 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.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Atlassian has defined an ERM process and conducts an enterprise risk assessment on an annual basis, which includes key product stakeholders.	Inquired of the control owner and ascertained that Atlassian had defined a risk management process, and conducted an enterprise risk assessment on an annual basis, inclusive of key product stakeholders.	No deviation noted.
	Inspected the ERM assessment and ascertained that Atlassian had defined an ERM process, and the enterprise risk assessment was performed on an annual basis, which includes key product stakeholders. Additionally, a monthly meeting was held to discuss updates to the enterprise risk assessment and results.	No deviation noted.
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.	Inquired of the control owner and ascertained that the Atlassian Risk and Compliance team evaluated the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Atlassian maintained a risk and controls matrix within their GRC tool.	No deviation noted.
	Inspected the GRC Tool used by Atlassian and ascertained that the Atlassian Risk and Compliance team evaluated the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Further ascertained that Atlassian maintained a risk and controls matrix within their GRC tool.	No deviation noted.
Internal audits are performed, results are communicated, and corrective actions are monitored.	Inquired of the Internal Audit and ascertained that internal audits were performed relating to SOX, ISO, SOC, and other operational audits. Further ascertained that results were communicated, and corrective actions were monitored.	No deviation noted.
	Inspected the GRC tool and Jira ticket and ascertained that internal audits were performed relating to SOX, ISO, SOC, and	No deviation noted.

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

CC 3.0 Common Criteria Related to Risk Assessment

CC 3.2 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.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	other operational audits. Further ascertained that results were communicated, and corrective actions were 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.	Inquired of the control owner and ascertained that the fraud risk assessment was performed on an annual basis by the Head of Risk and Compliance. Further ascertained that this included a survey of employees susceptible to fraud and evaluation of external risks. The results were evaluated by the Head of Risk and Compliance and included in the enterprise risk assessment communicated to the board and executive level managers annually.	No deviation noted.
	Inspected the most recent Enterprise Risk Management ("ERM") assessment and ascertained that Atlassian had defined an ERM process, and the enterprise risk assessment was performed on an annual basis, which includes key product stakeholders. Further ascertained that a fraud risk assessment was performed as part of the ERM assessment. Additionally, a monthly meeting was held to discuss updates to the enterprise and fraud risk assessment and results.	No deviation noted.

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

CC 3.0 Common Criteria Related to Risk Assessment

CC 3.2 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.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	Inspected the most recent fraud and enterprise risk assessment and ascertained that the assessment was performed and evaluated annually by the Head of Risk and Compliance. Further ascertained that a cross-functional survey of employees in areas susceptible to fraud was conducted and combined with an evaluation of external risks, and the results were included with the enterprise risk assessment. Additionally, ascertained that the results were communicated to the board and executive level managers as part of the annual meeting held.	The annual fraud risk assessment has not been completed during the audit period (November 1, 2019 to March 31, 2020). However, the Risk and Compliance Team performs fraud risk assessment as part of the periodic enterprise risk assessment.
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.	Inquired of the control owner and ascertained that incident management process was in place, the Site Reliability ("SRE") team was responsible for incidents and problems for Atlassian services and platforms, and that incident management process met the Atlassian Incident Management Standard. Further ascertained that for incidents with severity 0 and 1, a post incident review ("PIR") and root cause analysis were performed. Further ascertained that for incidents with security level 2 and 3, a post incident review express ("PIR-X") was performed.	No deviation noted.
	Inspected a sample of incidents and issues from the incident reporting and tracking system, and ascertained that incidents and issues were monitored and resolved timely. If Jira ticket corresponded to severity level 0 and 1, ascertained that post incident review ("PIR") and root cause analysis were performed. If a Jira ticket corresponded to severity level 2 and 3,	No deviation noted.

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

CC 3.0 Common Criteria Related to Risk Assessment

CC 3.2 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.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	ascertained that post incident review express ("PIR-X") was performed.	
Users (either internal or external) may report bugs, defects, or availability, security, and confidentiality issues via https://getsupport.atlassian.com, social media, general website forms, emails, https://trust.atlassian.com, and the public bug site.	Inquired of the control owner and ascertained that customers and internal users contacted Atlassian to report issues on bugs, defects, availability, security, and confidentiality via https://getsupport.atlassian.com, social media, general website forms, emails, https://trust.atlassian.com, and the public bug site.	No deviation noted.
	Inspected the channels of reporting for issues and ascertained that customers and internal users can contact Atlassian to report issues on bugs, defects, availability, security, and confidentiality via https://getsupport.atlassian.com, social media, general website forms, emails, https://trust.atlassian.com, and the public bug site.	No deviation noted.
	Inspected a sample of issues reported by either internal or external users, and ascertained that issues were followed up and resolved per incident management process.	No deviation noted.
Atlassian uses malware protection for Windows and OSX clients. An enterprise anti-malware platform provides endpoint protection, centralized reporting and notifications. The client is installed via management platforms and protected by a complex password	Inquired of the control owner and ascertained that malware protection for Windows and OSX clients was implemented and security patching was enforced on Windows endpoints. Additionally, complex password on the management platform prevent Windows and OSX clients from removing or uninstalling the agent.	No deviation noted.
	Inspected the configuration settings in the software used to enforce Malware protection and ascertained that malware protection was implemented and security patching was enforced on Windows endpoints.	No deviation noted.

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

CC 3.0 Common Criteria Related to Risk Assessment

CC 3.2 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.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
to prevent staff from removing or uninstalling the agent.	Attempted to uninstall the Malware protection software and ascertained that the malware protection was configured to prevent any users to uninstall the software.	No deviation noted.
IT Asset management software is used to monitor the hard drive encryption, user authentication requirements, and security patching are enforced on MacOS endpoints.	Inquired of the control owner and ascertained that IT asset management software was used for monitoring hard drive encryptions, user authentication requirements, and security patching on MacOS endpoints.	No deviation noted.
	Inspected the software used to enforce encryption and ascertained that IT Asset management software was used to monitor the hard drive encryption, user authentication requirements, and security patching was enforced on MacOS endpoints.	No deviation noted.
Penetration testing is performed by Bug Bounty on a continuous basis. Issues are reviewed and tracked to completion in a Jira ticket timely.	Inquired of the control owner and ascertained that penetration testing was performed by Bug Bounty on a continuous basis, and that issues were reviewed and tracked to completion in a Jira ticket by the Security team.	No deviation noted.
	Inspected the configuration of the BugCrowd application and observed that it ran on a continuous basis and issues were automatically created in a Jira ticket and tracked to completion by the Security team.	No deviation noted.
	Inspected a sample of issues identified from the penetration testing and ascertained that issues were reviewed and tracked to completion in a Jira ticket timely by the Security team.	No deviation noted.
Availability is published so that Customers may check the status/uptime of Statuspage.	Inquired of the control owner and ascertained that availability was published in the customer-facing website so that customers could check the status and uptime of Statuspage.	No deviation noted.

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

CC 3.0 Common Criteria Related to Risk Assessment

CC 3.2 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.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	Inspected the customer-facing website and ascertained that availability was published real-time, and the status and uptime metrics of Statuspage were communicated to customers.	No deviation noted.
Monitoring tools are in place to track and notify on the availability of Statuspage systems and services.	Inquired of the control owner and ascertained that Statuspage has monitoring tools in place to track and notify on the availability of Statuspage systems and services.	No deviation noted.
	Inspected the configuration of the monitoring tools in place and ascertained that monitoring tools were in place to monitor system availability of Statuspage systems and services.	No deviation noted.
	Inspected the configuration of the alert settings and ascertained that notifications were communicated to the appropriate Statuspage and Micros group.	No deviation noted.
	Inspected the resolution for a sample of HOT tickets created and ascertained that corrective actions were followed up and timely resolved.	No deviation noted.
Technical vulnerability management is implemented using vulnerability scanners. Critical threats are reviewed and resolved timely.	Inquired of the control owner and ascertained that technical vulnerability management was implemented using vulnerability scanners, and critical threats were reviewed and resolved by the security team in a timely manner.	No deviation noted.
	Inspected the configuration and tool used to monitor vulnerabilities and ascertained that technical vulnerability management was implemented using vulnerability scanners, and critical threats were reviewed and resolved timely by the security team.	No deviation noted.
	Inspected a sample of vulnerabilities identified from the vulnerability scanners and ascertained that incidents and issues were monitored and resolved timely by the security team.	No deviation noted.

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

CC 3.0 Common Criteria Related to Risk Assessment

CC 3.2 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.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Statuspage performs quarterly system-wide capacity audits to monitor utilization levels and adjust accordingly.	Inquired of the control owner and ascertained that system-wide capacity audits to monitor utilization levels were performed for Statuspage on a quarterly basis, and adjustments were made if necessary.	No deviation noted.
	Inspected a sample of quarterly review of the capacity audit results and ascertained that system-wide capacity reviews to monitor utilization levels were performed for Statuspage on a quarterly basis, and adjustments were made if necessary.	No deviation noted.

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

CC 3.0 Common Criteria Related to Risk Assessment

CC 3.3 The entity considers the potential for fraud in assessing risks to the achievement of objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
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.	Inquired of the control owner and ascertained that the fraud risk assessment was performed on an annual basis by the Head of Risk and Compliance. Further ascertained that this included a survey of employees susceptible to fraud and evaluation of external risks. The results were evaluated by the Head of Risk and Compliance and included in the enterprise risk assessment communicated to the board and executive level managers annually.	No deviation noted.
	Inspected the most recent Enterprise Risk Management ("ERM") assessment and ascertained that Atlassian had defined an ERM process, and the enterprise risk assessment was performed on an annual basis, which includes key product stakeholders. Further ascertained that a fraud risk assessment was performed as part of the ERM assessment. Additionally, a monthly meeting was held to discuss updates to the enterprise and fraud risk assessment and results.	No deviation noted.
	Inspected the most recent fraud and enterprise risk assessment and ascertained that the assessment was performed and evaluated annually by the Head of Risk and Compliance. Further ascertained that a cross-functional survey of employees in areas susceptible to fraud was conducted and combined with an evaluation of external risks, and the results were included with the enterprise risk assessment. Additionally, ascertained that the results were communicated to the board and executive level managers as part of the annual meeting held.	The annual fraud risk assessment has not been completed during the audit period (November 1, 2019 to March 31, 2020). However, the Risk and Compliance Team performs fraud risk assessment as part of the periodic enterprise risk assessment.

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

CC 3.0 Common Criteria Related to Risk Assessment

CC 3.4 The entity identifies and assesses changes that could significantly impact the system of internal control.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Audit Committee Charter defines roles, responsibilities, and key activities of the audit committee.	Inquired of the control owner and ascertained that Audit Committee Charter defines roles, responsibilities, and key activities of the audit committee.	No deviation noted.
	Inspected the Audit Committee Charter in the Atlassian's website and ascertained that roles, responsibilities, and key activities of the audit committee were defined.	No deviation noted.
Audit Committee Meeting calendar and general meeting agenda are developed.	Inquired of the control owner and ascertained that Audit Committee meeting calendar and general meeting agendas were developed.	No deviation noted.
	Inspected the Audit Committee latest notice for the annual general meeting and ascertained that Audit Committee meeting calendar and general meeting agendas were developed.	No deviation noted.
Qualifications for the Audit Committee's "Financial Expert" have been defined in the audit committee charter.	Inquired of the control owner and ascertained that the Audit Committee Charter defined the qualifications for the Audit Committee's "Financial Expert".	No deviation noted.
	Inspected the Audit Committee Charter in the Atlassian's website and ascertained that qualifications for the "Financial Expert" was defined.	No deviation noted.
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	Inquired of the control owner and ascertained that the Atlassian Risk and Compliance team evaluated the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Atlassian maintained a risk and controls matrix within their GRC tool.	No deviation noted.

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

CC 3.0 Common Criteria Related to Risk Assessment

CC 3.4 The entity identifies and assesses changes that could significantly impact the system of internal control.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
control environment. Atlassian maintains a risk and controls matrix within their GRC tool.	Inspected the GRC Tool used by Atlassian and ascertained that the Atlassian Risk and Compliance team evaluated the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Further ascertained that Atlassian maintained a risk and controls matrix within their GRC tool.	No deviation noted.
Vendor agreements, including any security, availability and confidentiality commitments, are reviewed during the procurement process.	Inquired of the control owner and ascertained that vendor agreements, including any security, availability, and confidentiality commitments, were reviewed during the procurement process.	No deviation noted.
	Inspected a sample of new vendors' third-party contracts and ascertained that the contracts included security, availability, and confidentiality commitments, and the contracts were executed between the third-party and Atlassian during the procurement process.	No deviation noted.

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

CC 4.0 Common Criteria Related to Monitoring Activities

CC 4.1 The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Atlassian has defined an ERM process and conducts an enterprise risk assessment on an annual basis, which includes key product stakeholders.	Inquired of the control owner and ascertained that Atlassian had defined a risk management process, and conducted an enterprise risk assessment on an annual basis, inclusive of key product stakeholders.	No deviation noted.
	Inspected the ERM assessment and ascertained that Atlassian had defined an ERM process, and the enterprise risk assessment was performed on an annual basis, which includes key product stakeholders. Additionally, a monthly meeting was held to discuss updates to the enterprise risk assessment and results.	No deviation noted.
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.	Inquired of the control owner and ascertained that the Atlassian Risk and Compliance team evaluated the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Atlassian maintained a risk and controls matrix within their GRC tool.	No deviation noted.
	Inspected the GRC Tool used by Atlassian and ascertained that the Atlassian Risk and Compliance team evaluated the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Further ascertained that Atlassian maintained a risk and controls matrix within their GRC tool.	No deviation noted.
Internal audits are performed, results are communicated, and corrective actions are monitored.	Inquired of the Internal Audit and ascertained that internal audits were performed relating to SOX, ISO, SOC, and other operational audits. Further ascertained that results were communicated, and corrective actions were monitored.	No deviation noted.
	Inspected the GRC tool and Jira ticket and ascertained that internal audits were performed relating to SOX, ISO, SOC, and	No deviation noted.

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

CC 4.0 Common Criteria Related to Monitoring Activities

CC 4.1 The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	other operational audits. Further ascertained that results were communicated, and corrective actions were monitored.	
At least annually, the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) have annually reviewed committee charters and corporate governance which define their roles, responsibilities, meeting frequency, participants, member qualifications, and discussion topics.	Inquired of the control owner and ascertained that the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) reviewed committee charters and corporate governance which defined their roles, responsibilities, meeting frequency, participants, member qualifications on an annual basis.	No deviation noted.
	Inspected the current year's Board of Directors and subcommittee annual meeting minutes, and ascertained that committee charters and corporate governance, which defined their roles, responsibilities, meeting frequency, participants, and member qualifications were discussed.	No deviation noted.

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

CC 4.0 Common Criteria Related to Monitoring Activities

CC 4.2 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.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Atlassian has defined an ERM process and conducts an enterprise risk assessment on an annual basis, which includes key product stakeholders.	Inquired of the control owner and ascertained that Atlassian had defined a risk management process, and conducted an enterprise risk assessment on an annual basis, inclusive of key product stakeholders.	No deviation noted.
	Inspected the ERM assessment and ascertained that Atlassian had defined an ERM process, and the enterprise risk assessment was performed on an annual basis, which includes key product stakeholders. Additionally, a monthly meeting was held to discuss updates to the enterprise risk assessment and results.	No deviation noted.
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.	Inquired of the control owner and ascertained that the Atlassian Risk and Compliance team evaluated the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Atlassian maintained a risk and controls matrix within their GRC tool.	No deviation noted.
	Inspected the GRC Tool used by Atlassian and ascertained that the Atlassian Risk and Compliance team evaluated the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Further ascertained that Atlassian maintained a risk and controls matrix within their GRC tool.	No deviation noted.
Internal audits are performed, results are communicated, and corrective actions are monitored.	Inquired of the Internal Audit and ascertained that internal audits were performed relating to SOX, ISO, SOC, and other operational audits. Further ascertained that results were communicated, and corrective actions were monitored.	No deviation noted.
	Inspected the GRC tool and Jira ticket and ascertained that internal audits were performed relating to SOX, ISO, SOC, and	No deviation noted.

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

CC 4.0 Common Criteria Related to Monitoring Activities

CC 4.2 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.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	other operational audits. Further ascertained that results were communicated, and corrective actions were monitored.	
At least annually, the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) have annually reviewed committee charters and corporate governance which define their roles, responsibilities, meeting frequency, participants, member qualifications, and discussion topics.	Inquired of the control owner and ascertained that the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) reviewed committee charters and corporate governance which defined their roles, responsibilities, meeting frequency, participants, member qualifications on an annual basis.	No deviation noted.
	Inspected the current year's Board of Directors and subcommittee annual meeting minutes, and ascertained that committee charters and corporate governance, which defined their roles, responsibilities, meeting frequency, participants, and member qualifications, were discussed.	No deviation noted.

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

CC 5.0 Common Criteria Related to Control Activities

CC 5.1 The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Atlassian has defined an ERM process and conducts an enterprise risk assessment on an annual basis, which includes key product stakeholders.	Inquired of the control owner and ascertained that Atlassian had defined a risk management process, and conducted an enterprise risk assessment on an annual basis, inclusive of key product stakeholders.	No deviation noted.
	Inspected the ERM assessment and ascertained that Atlassian had defined an ERM process, and the enterprise risk assessment was performed on an annual basis, which includes key product stakeholders. Additionally, a monthly meeting was held to discuss updates to the enterprise risk assessment and results.	No deviation noted.
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.	Inquired of the control owner and ascertained that the Atlassian Risk and Compliance team evaluated the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Atlassian maintained a risk and controls matrix within their GRC tool.	No deviation noted.
	Inspected the GRC Tool used by Atlassian and ascertained that the Atlassian Risk and Compliance team evaluated the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Further ascertained that Atlassian maintained a risk and controls matrix within their GRC tool.	No deviation noted.
Internal audits are performed, results are communicated, and corrective actions are monitored.	Inquired of the Internal Audit and ascertained that internal audits were performed relating to SOX, ISO, SOC, and other operational audits. Further ascertained that results were communicated, and corrective actions were monitored.	No deviation noted.
	Inspected the GRC tool and Jira ticket and ascertained that internal audits were performed relating to SOX, ISO, SOC, and	No deviation noted.

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

CC 5.0 Common Criteria Related to Control Activities

CC 5.1 The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	other operational audits. Further ascertained that results were communicated, and corrective actions were 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.	Inquired of the control owner and ascertained that the fraud risk assessment was performed on an annual basis by the Head of Risk and Compliance. Further ascertained that this included a survey of employees susceptible to fraud and evaluation of external risks. The results were evaluated by the Head of Risk and Compliance and included in the enterprise risk assessment communicated to the board and executive level managers annually.	No deviation noted.
	Inspected the most recent Enterprise Risk Management ("ERM") assessment and ascertained that Atlassian had defined an ERM process, and the enterprise risk assessment was performed on an annual basis, which includes key product stakeholders. Further ascertained that a fraud risk assessment was performed as part of the ERM assessment. Additionally, a monthly meeting was held to discuss updates to the enterprise and fraud risk assessment and results.	No deviation noted.

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

CC 5.0 Common Criteria Related to Control Activities

CC 5.1 The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.		
Controls Specified by Atlassian	Tests Performed by EY	Results of Tests
	Inspected the most recent fraud and enterprise risk assessment and ascertained that the assessment was performed and evaluated annually by the Head of Risk and Compliance. Further ascertained that a cross-functional survey of employees in areas susceptible to fraud was conducted and combined with an evaluation of external risks, and the results were included with the enterprise risk assessment. Additionally, ascertained that the results were communicated to the board and executive level managers as part of the annual meeting held.	The annual fraud risk assessment has not been completed during the audit period (November 1, 2019 to March 31, 2020). However, the Risk and Compliance Team performs fraud risk assessment as part of the periodic enterprise risk assessment.

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

CC 5.0 Common Criteria Related to Control Activities

CC 5.2 The entity also selects and develops general control activities over technology to support the achievement of objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Atlassian has defined an ERM process and conducts an enterprise risk assessment on an annual basis, which includes key product stakeholders.	Inquired of the control owner and ascertained that Atlassian had defined a risk management process, and conducted an enterprise risk assessment on an annual basis, inclusive of key product stakeholders.	No deviation noted.
	Inspected the ERM assessment and ascertained that Atlassian had defined an ERM process, and the enterprise risk assessment was performed on an annual basis, which includes key product stakeholders. Additionally, a monthly meeting was held to discuss updates to the enterprise risk assessment and results.	No deviation noted.
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.	Inquired of the control owner and ascertained that the Atlassian Risk and Compliance team evaluated the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Atlassian maintained a risk and controls matrix within their GRC tool.	No deviation noted.
	Inspected the GRC Tool used by Atlassian and ascertained that the Atlassian Risk and Compliance team evaluated the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Further ascertained that Atlassian maintained a risk and controls matrix within their GRC tool.	No deviation noted.
Internal audits are performed, results are communicated, and corrective actions are monitored.	Inquired of the Internal Audit and ascertained that internal audits were performed relating to SOX, ISO, SOC, and other operational audits. Further ascertained that results were communicated, and corrective actions were monitored.	No deviation noted.
	Inspected the GRC tool and Jira ticket and ascertained that internal audits were performed relating to SOX, ISO, SOC, and	No deviation noted.

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

CC 5.0 Common Criteria Related to Control Activities

CC 5.2 The entity also selects and develops general control activities over technology to support the achievement of objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	other operational audits. Further ascertained that results were communicated, and corrective actions were monitored.	
At least annually, the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) have annually reviewed committee charters and corporate governance which define their roles, responsibilities, meeting frequency, participants, member qualifications, and discussion topics.	Inquired of the control owner and ascertained that the Board of Directors and its various subcommittees (including Audit, Nominating and Governance, Compensation and Leadership Development) reviewed committee charters and corporate governance which defined their roles, responsibilities, meeting frequency, participants, member qualifications on an annual basis.	No deviation noted.
	Inspected the current year's Board of Directors and subcommittee annual meeting minutes, and ascertained that committee charters and corporate governance, which defined their roles, responsibilities, meeting frequency, participants, and member qualifications, were discussed.	No deviation noted.
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	Inquired of the control owner and ascertained that the fraud risk assessment was performed on an annual basis by the Head of Risk and Compliance. Further ascertained that this included a survey of employees susceptible to fraud and evaluation of external risks. The results were evaluated by the Head of Risk and Compliance and included in the enterprise risk assessment communicated to the board and executive level managers annually.	No deviation noted.

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

CC 5.0 Common Criteria Related to Control Activities

CC 5.2 The entity also selects and develops general control activities over technology to support the achievement of objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
a report. The results are included with the enterprise risk assessment which is communicated to the board and executive level managers annually.	Inspected the most recent Enterprise Risk Management ("ERM") assessment and ascertained that Atlassian had defined an ERM process, and the enterprise risk assessment was performed on an annual basis, which includes key product stakeholders. Further ascertained that a fraud risk assessment was performed as part of the ERM assessment. Additionally, a monthly meeting was held to discuss updates to the enterprise and fraud risk assessment and results.	No deviation noted.
	Inspected the most recent fraud and enterprise risk assessment and ascertained that the assessment was performed and evaluated annually by the Head of Risk and Compliance. Further ascertained that a cross-functional survey of employees in areas susceptible to fraud was conducted and combined with an evaluation of external risks, and the results were included with the enterprise risk assessment. Additionally, ascertained that the results were communicated to the board and executive level managers as part of the annual meeting held.	The annual fraud risk assessment has not been completed during the audit period (November 1, 2019 to March 31, 2020). However, the Risk and Compliance Team performs fraud risk assessment as part of the periodic enterprise risk assessment.

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

CC 5.0 Common Criteria Related to Control Activities

CC 5.3 The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Atlassian has defined an ERM process and conducts an enterprise risk assessment on an annual basis, which includes key product stakeholders.	Inquired of the control owner and ascertained that Atlassian had defined a risk management process, and conducted an enterprise risk assessment on an annual basis, inclusive of key product stakeholders.	No deviation noted.
	Inspected the ERM assessment and ascertained that Atlassian had defined an ERM process, and the enterprise risk assessment was performed on an annual basis, which includes key product stakeholders. Additionally, a monthly meeting was held to discuss updates to the enterprise risk assessment and results.	No deviation noted.
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.	Inquired of the control owner and ascertained that the Atlassian Risk and Compliance team evaluated the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Atlassian maintained a risk and controls matrix within their GRC tool.	No deviation noted.
	Inspected the GRC Tool used by Atlassian and ascertained that the Atlassian Risk and Compliance team evaluated the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Further ascertained that Atlassian maintained a risk and controls matrix within their GRC tool.	No deviation noted.
Internal audits are performed, results are communicated, and corrective actions are monitored.	Inquired of the Internal Audit and ascertained that internal audits were performed relating to SOX, ISO, SOC, and other operational audits. Further ascertained that results were communicated, and corrective actions were monitored.	No deviation noted.
	Inspected the GRC tool and Jira ticket and ascertained that internal audits were performed relating to SOX, ISO, SOC, and	No deviation noted.

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

CC 5.0 Common Criteria Related to Control Activities

CC 5.3 The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	other operational audits. Further ascertained that results were communicated, and corrective actions were monitored.	
Policies are posted and available online, assigned a policy owner, and reviewed at least annually by the designated policy owner or their delegate.	Inquired of the control owner and ascertained that policies were posted and available online, assigned a policy owner, and reviewed at least annually by the designated policy owner.	No deviation noted.
	Inspected the policies and ascertained that the policies were posted and available online, assigned a policy owner, and reviewed at least annually by the designated policy owner.	No deviation noted.
For every external offer that goes out, the manager or manager's manager will approve the offer or the HRIS team will approve on behalf of the manager if there is a peer or higher that has approved outside the system. The exception to this process is contractors, interns and graduates. • For contractors, who are hired outside of the standard hiring process, there is a confirmation of screening step in the onboarding process within Service Desk.	Inquired of the control owner and ascertained that for every external offer that goes out, the manager would approve the offer or the HRIS team would approve on behalf of the manager if there was a peer or higher that had approved outside the system. Further inquired and ascertained that for contractors, who were hired outside of the standard hiring process, there was a confirmation of screening step in the onboarding process within Service Desk. A recruiting manager would approve the offer letters for Interns and Grads because of the bulk nature and timing of these hires.	No deviation noted.
	Inspected a sample of job offers of new hires, interns, graduates, and contractors, and ascertained that job offers were reviewed and approved by a manager or confirmation of screening step in the onboarding process within Service Desk prior to hiring.	No deviation noted.

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

CC 5.0 Common Criteria Related to Control Activities

CC 5.3 The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
• A Recruiting Manager will approve the offer letters for Interns and Grads because of the bulk nature and timing of these hires.		
Performance appraisals are performed at least annually.	Inquired of the control owner and ascertained that performance appraisals were conducted at least annually.	No deviation noted.
	Inspected the performance appraisal results for a sample of employees and ascertained that performance appraisals were conducted at least annually.	The performance appraisals have not been performed during the audit period. The annual performance appraisals are performed between June and July annually. The last performance appraisals were performed in July 2019 and the next assessment is expected to be completed in July 2020.
Training is provided to employees to support their continued development and growth.	Inquired of the control owner and ascertained that employees are provided with the necessary training and support to continue to learn and grow.	No deviation noted.

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

CC 5.0 Common Criteria Related to Control Activities

CC 5.3 The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.		
Controls Specified by Atlassian	Tests Performed by EY	Results of Tests
	Inspected the training homepage and ascertained that training and support was provided to employees through the training homepage and employees can continue to learn and grow.	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Two-factor authentication is required when logging into VPN (Remote Access Service) from any IP address.	Inquired the control owner and ascertained that two-factor authentication was required when logging into VPN (Remote Access Service) from any IP address.	No deviation noted.
	Inspected the network configuration used on internal network endpoints and ascertained that two-factor authentication was required when logging into VPN (Remote Access Service) from any IP address.	No deviation noted.
	Attempted to access the VPN with and without the two-factor authentication and ascertained that two-factor authentication was required.	No deviation noted.
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.	Inquired of the control owner and ascertained that Duo integrates with Centrify to require two-factor authentication and Duo also extends two-factor protection to applications launched from a Centrify browser session. Further ascertained that Duo two-factor authentication was required when logging in from any IP that was not whitelisted within the "exempt IP" settings in Centrify.	No deviation noted.
	Inspected the configuration between Centrify and Duo and ascertained that two-factor authentication was enforced for all login attempts for non-Atlassian office networks or from any IP that was not whitelisted within the "exempt IP" settings in Centrify. Further inspected all IP addresses listed as exempt from Duo two-factor authentication and determined that these belong to Atlassian Office networks and verified that these were appropriate to be exempt from Duo two-factor authentication.	No deviation noted.
	Attempted to login to Centrify, any application from a Centrify browser session, and from an IP not whitelisted in Centrify, and	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	ascertained that two-factor authentication was required using Duo.	
Direct access to the Micros Platform via JumpBox requires a valid SSH key and two factor authentication.	Inquired of the control owner and ascertained that direct access to the Micros Platform via Jumpbox required a valid SSH key and Duo two-factor authentication.	No deviation noted.
	Inspected the network configuration and ascertained that direct access to the Micros Platform via Jumpbox required a valid SSH key and two-factor authentication.	No deviation noted.
	Attempted access to the Micros Platform via Jumpbox with and without a valid SSH key and ascertained that a valid SSH key and two-factor authentication was required.	No deviation noted
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.	Inquired of the control owner and ascertained that access to the Atlassian internal network and internal tools were 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.	No deviation noted.
	Inspected the configuration and ascertained that access to the Atlassian internal network and internal tools were 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.	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	Observed an Atlassian user accessing the internal network and internal tools, and ascertained that access was prohibited as the user was not assigned to the appropriate LDAP group or an active Active Directory account.	No deviation noted.
	Observed an Atlassian user accessing the internal network and internal tools, and ascertained that the user had an active Active Directory account and a member of an appropriate LDAP group.	No deviation noted.
Active Directory group membership is automatically assigned based on the user's department and team.	Inquired of the control owner and ascertained Active Directory group membership was automatically assigned based on the user's department and team.	No deviation noted.
	Inspected the configuration and ascertained that Active Directory group membership was automatically assigned based on the user's department and team in Workday.	No deviation noted.
	Inspected a sample user's Active Directory group membership and ascertained that it was based on the user's department and team in Workday.	No deviation noted.
Active Directory enforces password settings in line with the Atlassian Password Standard. Centrify Single Sign On allows users to have a single point of authentication to access multiple applications. Passwords settings for Centrify are enforced by Active Directory (AD) via the AD connector for Centrify.	Inquired of the control owner and ascertained that Centrify single sign-on allowed users to have a single point of authentication to access multiple applications and enforced minimum password length configured in Active Directory, which was in line with the Atlassian Password Standard.	No deviation noted.
	Observed a user login to Centrify and ascertained that single sign-on allowed users to have a single point of authentication to access multiple applications, and minimum password length was configured in Active Directory and enforced by Centrify which was in line with the Atlassian Password Standard.	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Privileged access to Deployment Bamboo is restricted to the members of the Build Engineering team.	Inquired of the control owner and ascertained that privileged access to Deployment Bamboo was restricted to the members of the Build Engineering team.	No deviation noted.
	Inspected the list of users with privileged access to Deployment Bamboo and ascertained that access was restricted to the members of the Build Engineering team.	No deviation noted.
Privileged access of Atlassian users to EC2 production environment is restricted to authorized and appropriate users only.	Inquired of the control owner and ascertained privileged access of Atlassian users to EC2 production environment was restricted to authorized and appropriate users only.	No deviation noted.
	Inspected the complete list of users with privileged access to EC2 production environment and ascertained that access was restricted to authorized and appropriate users only.	No deviation noted.
A Team Leader or Development Manager in Micros raises a Micros ticket to request access for user.	Inquired of the control owner and ascertained that Micros tickets were raised to request access for users.	No deviation noted.
	Inspected the Micros ticket for a sample of users granted access to the Micros platform and ascertained that a Micros ticket was raised to request access, appropriate approval was obtained prior to provisioning, and the access granted was per request.	No deviation noted.
Access is provisioned and approved as defined in Atlassian's SOP Policy.	Inquired of the control owner and ascertained that access to Statuspage systems was formally requested and approved prior to being provisioned, as defined in the Atlassian's Standard Operating Procedure ("SOP") relating to User Provisioning Requests.	No deviation noted.
	Inspected the request ticket for a sample of users granted access to Statuspage systems and ascertained that the access was approved as defined in the Atlassian's SOP Policy and prior to the provisioning of access. Further ascertained that the	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	access granted was the same as access requested and that access is appropriate based on user's job responsibilities.	
An automatic alert is triggered to the Risk and Compliance Manager and HR for any role change between the following groups: Engineering, Customer Support & Success (CSS), or Finance group. Appropriateness of access is reviewed and approved.	Inquired of the control owner and ascertained that an automatic alert was triggered to the Risk and Compliance Manager and HR for any role change between the following groups: Engineering, Customer Support and Success ("CSS"), or Finance group. Further ascertained that appropriateness of access was reviewed and approved.	No deviation noted.
	Inspected a sample of role changes between the Engineering, Customer Support and Success ("CSS"), or Finance group, and ascertained that an automatic alert was triggered to the Risk and Compliance Manager and HR, and appropriateness of access was reviewed and approved.	No deviation noted.
The HR system does not allow terminations to be backdated.	Inquired of the control owner and ascertained that HR system does not allow terminations to be backdated.	No deviation noted.
	Inspected the Workday configuration and ascertained that the HR system does not allow terminations to be backdated.	No deviation noted.
	Attempted to backdate an employee in Workday and ascertained that the HR system did not allow terminations to be backdated.	No deviation noted.
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.	Inquired the control owner and ascertained that 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	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
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.	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.	
	Inspected the job configured to run between Workday and Centrify and ascertained that the Active Directory account of terminated users were automatically suspended within up to eight (8) hours upon termination.	No deviation noted.
	Inspected the access removal date in Active Directory for a sampled terminated user and ascertained that access was removed timely for the sampled user.	No deviation noted.
	Inspected the SignalFX monitoring and history log of the Centrify job and ascertained that failure in the job was investigated and resolved timely.	No deviation noted.
The People Central Systems Support Specialist performs a review over Workday admin users semi-annually.	Inquired of the control owner and ascertained that the People Central Systems Support Specialist performed a review over Workday admin users semi-annually.	No deviation noted.
	Inspected a sampled user access review report over Workday Admin users and ascertained that the People Central Systems Support Specialist performed a review over Workday admin users on a semi-annual basis.	No deviation noted.
User access review is performed at least semi-annually for users with privileged access to Micros Platform and Databases and modification/removal is performed in a timely manner.	Inquired of the control owner and ascertained that user access reviews were conducted on a semi-annual basis for the Micros Platform and Databases and that removal were performed in a timely manner.	No deviation noted.
	Inspected a sampled user access review report and ascertained that it was performed on a semi-annual basis and that users with privileged access to Micros Platform and Databases are reviewed	Deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	and modified or removed access were actioned in a timely manner.	For one (1) semi-annual review of privileged access to the Micros Platform and Databases, evidence supporting the completeness and accuracy was not documented and retained.
Management Response: For the Micros user access review, evidence that the user listing was validated for completeness and accuracy was not included prior to the review being performed. Atlassian has updated their procedures and these requirements have been communicated to the Micros team, which will be reflected in the next semi-annual review. Additionally, there is an effective provisioning and deprovisioning control over user access to Micros that mitigates the risk of inappropriate access.		
On a semi-annual basis, a review of all privileged user accounts in the system, including shared, generic, and bot accounts is performed.	Inquired of the control owner and ascertained that the privileged access review, including shared/generic/bot accounts was performed on a semi-annual basis.	No deviation noted.
	Inspected a sampled user access review report over privileged access to Statuspage and supporting systems, and ascertained that the review was performed on a semi-annual basis and that privileged user access including shared, generic, bot accounts in Statuspage were reviewed and deemed appropriate.	No deviation noted.
On a semi-annual basis, the Build Engineering Development Team Lead performs a review of	Inquired of the control owner and ascertained that the Build Engineering Development Team Lead performed a review of privileged user access for Deployment bamboo semi-annually.	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
privileged user access for Deployment bamboo.	Inspected a sampled user access review report and ascertained that the Build Engineering Development Team Lead performed a review of privileged user access for Deployment bamboo semi-annually.	No deviation noted.
Access to customer data by the Statuspage Support team is supported by a valid customer support request.	Inquired of the control owner and ascertained that access to customer data by the Statuspage Support Team was supported by a valid customer support request.	No deviation noted.
	Inspected a sample of Statuspage Support team with access to customer data and ascertained that access was supported by a valid customer support request.	No deviation noted.
Statuspage assigns unique identifiers upon creation to customer data.	Inquired of the control owner and ascertained that Statuspage assigned unique identifiers upon creation of customer data.	No deviation noted.
	Inspected the Statuspage configuration and ascertained that all customers and users were configured to be provisioned with unique identifiers in Statuspage.	No deviation noted.
	Inspected a customer account and ascertained that a unique ID was assigned to the customer in the Statuspage production database.	No deviation noted.
External users securely connect to Statuspage via the encrypted SSL protocol.	Inquired of the control owner and ascertained the external users were connected to Statuspage using encrypted traffic via SSL protocol.	No deviation noted.
	Inspected the Statuspage webpage and ascertained the external users were connected to Statuspage using encrypted traffic via SSL protocol.	No deviation noted.
Statuspage data is encrypted at rest.	Inquired of the control owner and ascertained that Statuspage data was encrypted at rest.	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	Inspected the AWS encryption configuration and ascertained that Statuspage data was encrypted at rest.	No deviation noted.
Atlassian uses malware protection for Windows and OSX clients. An enterprise anti-malware platform provides endpoint protection, centralized reporting and notifications. The client is installed via management platforms and protected by a complex password to prevent staff from removing or uninstalling the agent.	Inquired of the control owner and ascertained that malware protection for Windows and OSX clients was implemented and security patching was enforced on Windows endpoints. Additionally, complex password on the management platform prevent Windows and OSX clients from removing or uninstalling the agent.	No deviation noted.
	Inspected the configuration settings in the software used to enforce Malware protection and ascertained that malware protection was implemented and security patching was enforced on Windows endpoints.	No deviation noted.
	Attempted to uninstall the Malware protection software and ascertained that the malware protection was configured to prevent any users to uninstall the software.	No deviation noted.
IT Asset management software is used to monitor the hard drive encryption, user authentication requirements, and security patching are enforced on MacOS endpoints.	Inquired of the control owner and ascertained that IT asset management software was used for monitoring hard drive encryptions, user authentication requirements, and security patching on MacOS endpoints.	No deviation noted.
	Inspected the software used to enforce encryption and ascertained that IT Asset management software was used to monitor the hard drive encryption, user authentication requirements, and security patching was enforced on MacOS endpoints.	No deviation noted.
IT Asset management software is used to monitor hard drive	Inquired of the control owner and ascertained that IT asset management software was used for monitoring hard drive	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
encryption, user authentication requirements, and security patching on Windows endpoints.	encryptions, user authentication requirements, and security patching on Windows endpoints.	
	Inspected the software used to enforce encryption and ascertained that IT Asset management software was used to monitor the hard drive encryption, user authentication requirements, and security patching was enforced on Windows endpoints.	No deviation noted.
Atlassian reviews the SOC reports of the vendors on an annual basis.	Inquired of the control owner and ascertained that Atlassian reviewed the SOC reports of the vendors ("subservice organizations") on an annual basis.	No deviation noted.
	Inspected the Jira ticket for the review of the SOC 2 or equivalent attestation reports and ascertained that leadership reviewed the reports annually. Reviews included an assessment of complementary user entity controls, subservice organizations, and mapping of the controls to key risks. If there were exceptions, Atlassian reviewed the severity and impact of the exceptions, and if needed, followed-up with the individual vendor.	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Two-factor authentication is required when logging into VPN (Remote Access Service) from any IP address.	Inquired the control owner and ascertained that two-factor authentication was required when logging into VPN (Remote Access Service) from any IP address.	No deviation noted.
	Inspected the network configuration used on internal network endpoints and ascertained that two-factor authentication was required when logging into VPN (Remote Access Service) from any IP address.	No deviation noted.
	Attempted to access the VPN with and without the two-factor authentication and ascertained that two-factor authentication was required.	No deviation noted.
Active Directory enforces password settings in line with the Atlassian Password Standard. Centrify Single Sign On allows users to have a single point of authentication to access multiple applications. Passwords settings for Centrify are enforced by Active Directory (AD) via the AD connector for Centrify.	Inquired of the control owner and ascertained that Centrify single sign-on allowed users to have a single point of authentication to access multiple applications and enforced minimum password length configured in Active Directory, which was in line with the Atlassian Password Standard.	No deviation noted.
	Observed a user login to Centrify and ascertained that single sign-on allowed users to have a single point of authentication to access multiple applications, and minimum password length was configured in Active Directory and enforced by Centrify which was in line with the Atlassian Password Standard.	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
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.	Inquired of the control owner and ascertained that access to the Atlassian internal network and internal tools were 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.	No deviation noted.
	Inspected the configuration and ascertained that access to the Atlassian internal network and internal tools were 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.	No deviation noted.
	Observed an Atlassian user getting access to the internal network and internal tools, and ascertained that access was prohibited as the user was not assigned to the appropriate LDAP group or an active Active Directory account.	No deviation noted.
	Observed an Atlassian user getting access to the internal network and internal tools, and ascertained that the user had an active Active Directory account and a member of an appropriate LDAP group.	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Direct access to the Micros Platform via JumpBox requires a valid SSH key and two factor authentication.	Inquired of the control owner and ascertained that direct access to the Micros Platform via Jumpbox required a valid SSH key and Duo two-factor authentication.	No deviation noted.
	Inspected the network configuration and ascertained that direct access to the Micros Platform via Jumpbox required a valid SSH key and two-factor authentication.	No deviation noted.
	Attempted access the Micros Platform via Jumpbox with and without a valid SSH key and ascertained that a valid SSH key and two-factor authentication was required.	No deviation noted.
Privileged access to Deployment Bamboo is restricted to the members of the Build Engineering team.	Inquired of the control owner and ascertained that privileged access to Deployment Bamboo was restricted to the members of the Build Engineering team.	No deviation noted.
	Inspected the list of users with privileged access to Deployment Bamboo and ascertained that access was restricted to the members of the Build Engineering team.	No deviation noted.
Privileged access of Atlassian users to EC2 production environment is restricted to authorized and appropriate users only.	Inquired of the control owner and ascertained privileged access of Atlassian users to EC2 production environment was restricted to authorized and appropriate users only.	No deviation noted.
	Inspected the complete list of users with privileged access to EC2 production environment and ascertained that access was restricted to authorized and appropriate users only.	No deviation noted.
Access is provisioned and approved as defined in Atlassian's SOP Policy.	Inquired of the control owner and ascertained that access to Statuspage systems was formally requested and approved prior to being provisioned, as defined in the Atlassian's Standard Operating Procedure ("SOP") relating to User Provisioning Requests.	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	Inspected the request ticket for a sample of users granted access to Statuspage systems and ascertained that the access was approved as defined in the Atlassian's SOP Policy and prior to the provisioning of access. Further ascertained that the access granted was the same as access requested, and that access is appropriate based on user's job responsibilities.	No deviation noted.
A Team Leader or Development Manager in Micros raises a Micros ticket to request access for user.	Inquired of the control owner and ascertained that Micros tickets were raised to request access for users.	No deviation noted.
	Inspected the Micros ticket for a sample of users granted access to the Micros platform and ascertained that a Micros ticket was raised to request access, appropriate approval was obtained prior to provisioning, and the access granted was per request.	No deviation noted.
An automatic alert is triggered to the Risk and Compliance Manager and HR for any role change between the following groups: Engineering, Customer Support & Success (CSS), or Finance group. Appropriateness of access is reviewed and approved.	Inquired of the control owner and ascertained that an automatic alert was triggered to the Risk and Compliance Manager and HR for any role change between the following groups: Engineering, Customer Support and Success ("CSS"), or Finance group. Further ascertained that appropriateness of access was reviewed and approved.	No deviation noted.
	Inspected a sample of role changes between the Engineering, Customer Support and Success ("CSS"), or Finance group, and ascertained that an automatic alert was triggered to the Risk and Compliance Manager and HR, and appropriateness of access was reviewed and approved.	No deviation noted.
The HR system does not allow terminations to be backdated.	Inquired of the control owner and ascertained that HR system does not allow terminations to be backdated.	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	Inspected the Workday configuration and ascertained that the HR system does not allow terminations to be backdated.	No deviation noted.
	Attempted to backdate an employee in Workday and ascertained that the HR system did not allow terminations to be backdated.	No deviation noted.
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.	Inquired the control owner and ascertained that 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.	No deviation noted.
	Inspected the job configured to run between Workday and Centrify and ascertained that the Active Directory account of terminated users were automatically suspended within up to eight (8) hours upon termination.	No deviation noted.
	Inspected the access removal date in Active Directory for a sampled terminated user and ascertained that access was removed timely for the sampled user.	No deviation noted.
	Inspected the SignalFX monitoring and history log of the Centrify job and ascertained that failure in the job was investigated and resolved timely.	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
The People Central Systems Support Specialist performs a review over Workday admin users semi-annually.	Inquired of the control owner and ascertained that the People Central Systems Support Specialist performed a review over Workday admin users semi-annually.	No deviation noted.
	Inspected a sampled user access review report over Workday Admin users and ascertained that the People Central Systems Support Specialist performed a review over Workday admin users on a semi-annual basis.	No deviation noted.
User access review is performed at least semi-annually for users with privileged access to Micros Platform and Databases and modification/removal is performed in a timely manner.	Inquired of the control owner and ascertained that user access reviews were conducted on a semi-annual basis for the Micros Platform and Databases and that removal were performed in a timely manner.	No deviation noted.
	Inspected a sampled user access review report and ascertained that it was performed on a semi-annual basis and that users with privileged access to Micros Platform and Databases are reviewed and modified or removed access were actioned in a timely manner.	Deviation noted. For one (1) semi-annual review of privileged access to the Micros Platform and Databases, evidence supporting the completeness and accuracy was not documented and retained.
Management Response: For the Micros user access review, evidence that the user listing was validated for completeness and accuracy was not included prior to the review being performed. Atlassian has updated their procedures and these requirements have been communicated		

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
to the Micros team, which will be reflected in the next semi-annual review. Additionally, there is an effective provisioning and deprovisioning control over user access to Micros that mitigates the risk of inappropriate access.		
On a semi-annual basis, a review of all privileged user accounts in the system, including shared, generic, and bot accounts is performed.	Inquired of the control owner and ascertained that the privileged access review, including shared/generic/bot accounts was performed on a semi-annual basis.	No deviation noted.
	Inspected a sampled user access review report over privileged access to Statuspage and supporting systems, and ascertained that the review was performed on a semi-annual basis and that privileged user access including shared, generic, bot accounts in Statuspage were reviewed and deemed appropriate.	No deviation noted.
On a semi-annual basis, the Build Engineering Development Team Lead performs a review of privileged user access for Deployment bamboo.	Inquired of the control owner and ascertained that the Build Engineering Development Team Lead performed a review of privileged user access for Deployment bamboo semi-annually.	No deviation noted.
	Inspected a sampled user access review report and ascertained that the Build Engineering Development Team Lead performed a review of privileged user access for Deployment bamboo semi-annually.	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Direct access to the Micros Platform via JumpBox requires a valid SSH key and two factor authentication.	Inquired of the control owner and ascertained that direct access to the Micros Platform via Jumpbox required a valid SSH key and Duo two-factor authentication.	No deviation noted.
	Inspected the network configuration and ascertained that direct access to the Micros Platform via Jumpbox required a valid SSH key and two-factor authentication.	No deviation noted.
	Attempted access to the Micros Platform via Jumpbox with and without a valid SSH key and ascertained that a valid SSH key and two-factor authentication was required.	No deviation noted.
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.	Inquired of the control owner and ascertained that access to the Atlassian internal network and internal tools were 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.	No deviation noted.
	Inspected the configuration and ascertained that access to the Atlassian internal network and internal tools were 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.	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	Observed an Atlassian user getting access to the internal network and internal tools, and ascertained that access was prohibited as the user was not assigned to the appropriate LDAP group or an active Active Directory account.	No deviation noted.
	Observed an Atlassian user getting access to the internal network and internal tools, and ascertained that the user had an active Active Directory account and a member of an appropriate LDAP group.	No deviation noted.
Active Directory group membership is automatically assigned based on the user's department and team.	Inquired of the control owner and ascertained Active Directory group membership was automatically assigned based on the user's department and team.	No deviation noted.
	Inspected the configuration and ascertained that Active Directory group membership was automatically assigned based on the user's department and team in Workday.	No deviation noted.
	Inspected a sample user's Active Directory group membership and ascertained that it was based on the user's department and team in Workday.	No deviation noted.
Privileged access to Deployment Bamboo is restricted to the members of the Build Engineering team.	Inquired of the control owner and ascertained that privileged access to Deployment Bamboo was restricted to the members of the Build Engineering team.	No deviation noted.
	Inspected the list of users with privileged access to Deployment Bamboo and ascertained that access was restricted to the members of the Build Engineering team.	No deviation noted.
Privileged access of Atlassian users to EC2 production environment is restricted to	Inquired of the control owner and ascertained privileged access of Atlassian users to EC2 production environment was restricted to authorized and appropriate users only.	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
authorized and appropriate users only.	Inspected the complete list of users with privileged access to EC2 production environment and ascertained that access was restricted to authorized and appropriate users only.	No deviation noted.
A Team Leader or Development Manager in Micros raises a Micros ticket to request access for user.	Inquired of the control owner and ascertained that Micros tickets were raised to request access for users.	No deviation noted.
	Inspected the Micros ticket for a sample of users granted access to the Micros platform and ascertained that a Micros ticket was raised to request access, appropriate approval was obtained prior to provisioning, and the access granted was per request.	No deviation noted.
Access is provisioned and approved as defined in Atlassian's SOP Policy.	Inquired of the control owner and ascertained that access to Statuspage systems was formally requested and approved prior to being provisioned, as defined in the Atlassian's Standard Operating Procedure ("SOP") relating to User Provisioning Requests.	No deviation noted.
	Inspected the request ticket for a sample of users granted access to Statuspage systems and ascertained that the access was approved as defined in the Atlassian's SOP Policy and prior to the provisioning of access. Further ascertained that the access granted was the same as access requested, and that access is appropriate based on user's job responsibilities.	No deviation noted.
An automatic alert is triggered to the Risk and Compliance Manager and HR for any role change between the following groups: Engineering, Customer Support & Success (CSS), or Finance group.	Inquired of the control owner and ascertained that an automatic alert was triggered to the Risk and Compliance Manager and HR for any role change between the following groups: Engineering, Customer Support and Success ("CSS"), or Finance group. Further ascertained that appropriateness of access was reviewed and approved.	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Appropriateness of access is reviewed and approved.	Inspected a sample of role changes between the Engineering, Customer Support and Success ("CSS"), or Finance group, and ascertained that an automatic alert was triggered to the Risk and Compliance Manager and HR, and appropriateness of access was reviewed and approved.	No deviation noted.
The People Central Systems Support Specialist performs a review over Workday admin users semi-annually.	Inquired of the control owner and ascertained that the People Central Systems Support Specialist performed a review over Workday admin users semi-annually.	No deviation noted.
	Inspected a sampled user access review report over Workday Admin users and ascertained that the People Central Systems Support Specialist performed a review over Workday admin users on a semi-annual basis.	No deviation noted.
User access review is performed at least semi-annually for users with privileged access to Micros Platform and Databases and modification/removal is performed in a timely manner.	Inquired of the control owner and ascertained that user access reviews were conducted on a semi-annual basis for the Micros Platform and Databases and that removal were performed in a timely manner.	No deviation noted.
	Inspected a sampled user access review report and ascertained that it was performed on a semi-annual basis and that users with privileged access to Micros Platform and Databases are reviewed and modified or removed access were actioned in a timely manner.	Deviation noted. For one (1) semi-annual review of privileged access to the Micros Platform and Databases, evidence supporting the completeness and accuracy was not documented and retained.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Management Response: For the Micros user access review, evidence that the user listing was validated for completeness and accuracy was not included prior to the review being performed. Atlassian has updated their procedures and these requirements have been communicated to the Micros team, which will be reflected in the next semi-annual review. Additionally, there is an effective provisioning and deprovisioning control over user access to Micros that mitigates the risk of inappropriate access.		
On a semi-annual basis, a review of all privileged user accounts in the system, including shared, generic, and bot accounts is performed.	Inquired of the control owner and ascertained that the privileged access review, including shared/generic/bot accounts was performed on a semi-annual basis.	No deviation noted.
	Inspected a sampled user access review report over privileged access to Statuspage and supporting systems, and ascertained that the review was performed on a semi-annual basis and that privileged user access including shared, generic, bot accounts in Statuspage were reviewed and deemed appropriate.	No deviation noted.
On a semi-annual basis, the Build Engineering Development Team Lead performs a review of privileged user access for Deployment bamboo.	Inquired of the control owner and ascertained that the Build Engineering Development Team Lead performed a review of privileged user access for Deployment bamboo semi-annually.	No deviation noted.
	Inspected a sampled user access review report and ascertained that the Build Engineering Development Team Lead performed a review of privileged user access for Deployment bamboo semi-annually.	No deviation noted.
Access to customer data by the Statuspage Support team is	Inquired of the control owner and ascertained that access to customer data by the Statuspage Support Team was supported by a valid customer support request.	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
supported by a valid customer support request.	Inspected a sample of Statuspage Support team with access to customer data and ascertained that access was supported by a valid customer support request.	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.4 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.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Atlassian reviews the SOC report of the vendor on an annual basis.	Inquired of the control owner and ascertained that Atlassian reviewed the SOC reports of the vendors ("subservice organizations") on an annual basis.	No deviation noted.
	Inspected the Jira ticket for the review of the SOC 2 or equivalent attestation reports and ascertained that leadership reviewed the reports annually. Reviews included an assessment of complementary user entity controls, subservice organizations, and mapping of the controls to key risks. If there were exceptions, Atlassian reviewed the severity and impact of the exceptions, and if needed, followed-up with the individual vendor.	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Atlassian reviews the SOC report of the vendor on an annual basis.	Inquired of the control owner and ascertained that Atlassian reviewed the SOC reports of the vendors ("subservice organizations") on an annual basis.	No deviation noted.
	Inspected the Jira ticket for the review of the SOC 2 or equivalent attestation reports and ascertained that leadership reviewed the reports annually. Reviews included an assessment of complementary user entity controls, subservice organizations, and mapping of the controls to key risks. If there were exceptions, Atlassian reviewed the severity and impact of the exceptions, and if needed, followed-up with the individual vendor.	No deviation noted.
Statuspage data is deleted within 30 days of receipt of a request for deletion.	Inquired of the control owner and ascertained that Statuspage data was deleted within 30 days of receipt of a request for deletion.	No deviation noted.
	Inspected the Statuspage database for a sample of customers and ascertained that Statuspage data was deleted within 30 days of receipt of a request for deletion.	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Two-factor authentication is required when logging into VPN (Remote Access Service) from any IP address.	Inquired the control owner and ascertained that two-factor authentication was required when logging into VPN (Remote Access Service) from any IP address.	No deviation noted.
	Inspected the network configuration used on internal network endpoints and ascertained that two-factor authentication was required when logging into VPN (Remote Access Service) from any IP address.	No deviation noted.
	Attempted to access the VPN with and without the two-factor authentication and ascertained that two-factor authentication was required.	No deviation noted.
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.	Inquired of the control owner and ascertained that Duo integrates with Centrify to require two-factor authentication and Duo also extends two-factor protection to applications launched from a Centrify browser session. Further ascertained that Duo two-factor authentication was required when logging in from any IP that was not whitelisted within the "exempt IP" settings in Centrify.	No deviation noted.
	Inspected the configuration between Centrify and Duo and ascertained that two-factor authentication was enforced for all login attempts for non-Atlassian office networks or from any IP that was not whitelisted within the "exempt IP" settings in Centrify. Further inspected all IP addresses listed as exempt from Duo two-factor authentication and determined that these belong to Atlassian Office networks and verified that these were appropriate to be exempt from Duo two-factor authentication.	No deviation noted.
	Attempted to login to Centrify, any application from a Centrify browser session, and from an IP not whitelisted in Centrify, and	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	ascertained that two-factor authentication was required using Duo.	
Active Directory enforces password settings in line with the Atlassian Password Standard. Centrify Single Sign On allows users to have a single point of authentication to access multiple applications. Passwords settings for Centrify are enforced by Active Directory (AD) via the AD connector for Centrify.	Inquired of the control owner and ascertained that Centrify single sign-on allowed users to have a single point of authentication to access multiple applications and enforced minimum password length configured in Active Directory, which was in line with the Atlassian Password Standard.	No deviation noted.
	Observed a user login to Centrify and ascertained that single sign-on allowed users to have a single point of authentication to access multiple applications, and minimum password length was configured in Active Directory and enforced by Centrify which was in line with the Atlassian Password Standard.	No deviation noted.
Access to the Atlassian internal network and internal tools is restricted to authorized users via logical access measures:	Inquired of the control owner and ascertained that access to the Atlassian internal network and internal tools were 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.	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
• Each Atlassian user must have an active Active Directory account. • Each Atlassian user must be members of the appropriate LDAP group.	Inspected the configuration and ascertained that access to the Atlassian internal network and internal tools were 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.	No deviation noted.
	Observed an Atlassian user getting access to the internal network and internal tools, and ascertained that access was prohibited as the user was not assigned to the appropriate LDAP group or an active Active Directory account.	No deviation noted.
	Observed an Atlassian user getting access to the internal network and internal tools, and ascertained that the user had an active Active Directory account and a member of an appropriate LDAP group.	No deviation noted.
Direct access to the Micros Platform via JumpBox requires a valid SSH key and two factor authentication.	Inquired of the control owner and ascertained that direct access to the Micros Platform via Jumpbox required a valid SSH key and Duo two-factor authentication.	No deviation noted.
	Inspected the network configuration and ascertained that direct access to the Micros Platform via Jumpbox required a valid SSH key and two-factor authentication.	No deviation noted.
	Attempted access to the Micros Platform via Jumpbox with and without a valid SSH key and ascertained that a valid SSH key and two-factor authentication was required.	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
External users securely connect to Statuspage via the encrypted SSL protocol.	Inquired of the control owner and ascertained the external users were connected to Statuspage using encrypted traffic via SSL protocol.	No deviation noted.
	Inspected the Statuspage webpage and ascertained the external users were connected to Statuspage using encrypted traffic via SSL protocol.	No deviation noted.
Firewall rules are in place to restrict access to the production environment.	Inquired of the control owner and ascertained firewall rules were in place to restrict access to the production environment.	No deviation noted.
	Inspected the security policy settings and the configurations set up in the network, and ascertained firewall rules were in place to restrict access to the production environment.	No deviation noted.
Production data is not used in non-production environments and must be protected in alignment with Atlassian's System Acquisition, Development, and Maintenance Policy.	Inquired of the control owner and ascertained that production data was not used in non-production environments, and must be protected in alignment with Atlassian's System Acquisition, Development, and Maintenance Policy.	No deviation noted.
	Inspected a customer's production data in the non-production environment and ascertained that the customer's production data did not exist in the non-production environment.	No deviation noted.
Statuspage assigns unique identifiers upon creation to customer data.	Inquired of the control owner and ascertained that Statuspage assigned unique identifiers upon creation of customer data.	No deviation noted.
	Inspected the Statuspage configuration and ascertained that all customers and users were configured to be provisioned with unique identifiers in Statuspage.	No deviation noted.
	Inspected a customer account and ascertained that a unique ID was assigned to the customer in the Statuspage production database.	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
External users securely connect to Statuspage via the encrypted SSL protocol.	Inquired of the control owner and ascertained the external users were connected to Statuspage using encrypted traffic via SSL protocol.	No deviation noted.
	Inspected the Statuspage webpage and ascertained the external users were connected to Statuspage using encrypted traffic via SSL protocol.	No deviation noted.
Statuspage data is encrypted at rest.	Inquired of the control owner and ascertained that Statuspage data was encrypted at rest.	No deviation noted.
	Inspected the AWS encryption configuration and ascertained that Statuspage data was encrypted at rest.	No deviation noted.
Statuspage assigns unique identifiers upon creation to customer data.	Inquired of the control owner and ascertained that Statuspage assigned unique identifiers upon creation of customer data.	No deviation noted.
	Inspected the Statuspage configuration and ascertained that all customers and users were configured to be provisioned with unique identifiers in Statuspage.	No deviation noted.
	Inspected a customer account and ascertained that a unique ID was assigned to the customer in the Statuspage production database.	No deviation noted.
Production data is not used in non-production environments and must be protected in alignment with Atlassian's System Acquisition, Development, and Maintenance Policy.	Inquired of the control owner and ascertained that production data was not used in non-production environments, and must be protected in alignment with Atlassian's System Acquisition, Development, and Maintenance Policy.	No deviation noted.
	Inspected a customer's production data in the non-production environment and ascertained that the customer's production data did not exist in the non-production environment.	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Statuspage data is deleted within 30 days of receipt of a request for deletion.	Inquired of the control owner and ascertained that Statuspage data was deleted within 30 days of receipt of a request for deletion.	No deviation noted.
	Inspected the Statuspage database for a sample of customers and ascertained that Statuspage data was deleted within 30 days of receipt of a request for deletion.	No deviation noted.
Atlassian uses malware protection for Windows and OSX clients. An enterprise anti-malware platform provides endpoint protection, centralized reporting and notifications. The client is installed via management platforms and protected by a complex password to prevent staff from removing or uninstalling the agent.	Inquired of the control owner and ascertained that malware protection for Windows and OSX clients was implemented and security patching was enforced on Windows endpoints. Additionally, complex password on the management platform prevent Windows and OSX clients from removing or uninstalling the agent.	No deviation noted.
	Inspected the configuration settings in the software used to enforce Malware protection and ascertained that malware protection was implemented and security patching was enforced on Windows endpoints.	No deviation noted.
	Attempted to uninstall the Malware protection software and ascertained that the malware protection was configured to prevent any users to uninstall the software.	No deviation noted.
IT Asset management software is used to monitor the hard drive encryption, user authentication requirements, and security	Inquired of the control owner and ascertained that IT asset management software was used for monitoring hard drive encryptions, user authentication requirements, and security patching on MacOS endpoints.	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
patching are enforced on MacOS endpoints.	Inspected the software used to enforce encryption and ascertained that IT Asset management software was used to monitor the hard drive encryption, user authentication requirements, and security patching was enforced on MacOS endpoints.	No deviation noted.
IT Asset management software is used to monitor hard drive encryption, user authentication requirements, and security patching on Windows endpoints.	Inquired of the control owner and ascertained that IT asset management software was used for monitoring hard drive encryptions, user authentication requirements, and security patching on Windows endpoints.	No deviation noted.
	Inspected the software used to enforce encryption and ascertained that IT Asset management software was used to monitor the hard drive encryption, user authentication requirements, and security patching was enforced on Windows endpoints.	No deviation noted.
Code scanning is performed by SourceClear on a continuous basis for Statuspage.	Inquired of the control owner and ascertained that code scanning was performed by SourceClear on a continuous basis on Statuspage's source code to identify potential vulnerabilities.	No deviation noted.
	Inspected the SourceClear configuration and ascertained that code scanning was performed by SourceClear on a continuous basis on Statuspage's source code to identify potential vulnerabilities.	No deviation noted.
	Inspected a sample of vulnerabilities identified from the code scanning through SourceClear and ascertained that vulnerabilities were reviewed by appropriate Atlassian management and tracked to completion timely.	No deviation noted.
Users (either internal or external) may report bugs, defects, or	Inquired of the control owner and ascertained that customers and internal users contacted Atlassian to report issues on bugs,	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
availability, security, and confidentiality issues via https://getsupport.atlassian.com, social media, general website forms, emails, https://trust.atlassian.com, and the public bug site.	defects, availability, security, and confidentiality via https://getsupport.atlassian.com, social media, general website forms, emails, https://trust.atlassian.com, and the public bug site.	
	Inspected the channels of reporting for issues and ascertained that customers and internal users can contact Atlassian to report issues on bugs, defects, availability, security, and confidentiality via https://getsupport.atlassian.com, social media, general website forms, emails, https://trust.atlassian.com, and the public bug site.	No deviation noted.
	Inspected a sample of issues reported by either internal or external users, and ascertained that issues were followed up and resolved per incident management process.	No deviation noted.
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.	Inquired of the control owner and ascertained that incident management process was in place, the Site Reliability ("SRE") team was responsible for incidents and problems for Atlassian services and platforms, and that incident management process met the Atlassian Incident Management Standard. Further ascertained that for incidents with severity 0 and 1, a post incident review ("PIR") and root cause analysis were performed. Further ascertained that for incidents with security level 2 and 3, a post incident review express ("PIR-X") was performed.	No deviation noted.
	Inspected a sample of incidents and issues from the incident reporting and tracking system, and ascertained that incidents and issues were monitored and resolved timely. If Jira ticket corresponded to severity level 0 and 1, ascertained that post incident review ("PIR") and root cause analysis were performed.	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	If a Jira ticket corresponded to severity level 2 and 3, ascertained that post incident review express ("PIR-X") was performed.	
Firewall rules are in place to restrict access to the production environment.	Inquired of the control owner and ascertained firewall rules were in place to restrict access to the production environment.	No deviation noted.
	Inspected the security policy settings and the configurations set up in the network, and ascertained firewall rules were in place to restrict access to the production environment.	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
The Micros platform will not allow code artefacts to deploy or run on the platform unless they have been peer reviewed and have passed green build testing.	Inquired of the control owner and ascertained that changes were documented through pull requests, and peer review and passed green build testing was required prior to merging the code to the master branch.	No deviation noted.
	Inspected the Bitbucket configuration and ascertained that changes were documented through pull requests, and that the Bitbucket repositories would not allow changes to deploy or run on the platform unless they have been peer reviewed and have passed green build testing.	No deviation noted.
	Inspected a sample of merged pull requests and ascertained that documented peer review and green build testing was required prior to merging the code to master branch.	No deviation noted.
Micros will only pull deployment artefacts from the restricted namespace. Only deployment-bamboo has the credentials to push to the restricted namespace.	Inquired of the control owner and ascertained that artefacts with peer review and passed green build testing were deployed from a restricted namespace by deployment-bamboo bot account.	No deviation noted.
	Inspected the list of accounts with ability to commit changes to Docker and ascertained that only deployment-bamboo was assigned to push changes to Docker.	No deviation noted.
	Attempted to push a change to the restricted Docker namespace using an end user account and ascertained that the deployed change was denied.	No deviation noted.
Bitbucket does not allow a pull request to be approved by the same user who requests it.	Inquired of the control owner and ascertained that Bitbucket does not allow a pull requests to be approved by the same user who requests it.	No deviation noted.
	Attempted a creation of pull request and ascertained that Bitbucket did not allow a pull request to be approved by the same user who requested it.	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	Inspected a sample of merged pull requests and ascertained that the peer reviewer requester was not the same as the approver.	No deviation noted.
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.	Inquired of the control owner and ascertained that Bamboo would not allow code to be deployed unless it has passed green build testing.	No deviation noted.
	Attempted to deploy a red build code and ascertained that it did not allow the code to be deployed unless it has passed green build testing.	No deviation noted.
	Attempted to deploy a green build code and ascertained that Bamboo allowed the code to be deployed.	No deviation noted.
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 were not enforced, the code is rejected.	Inquired of the control owner and ascertained that 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.	No deviation noted.
	Inspected the API configuration in Deployment bamboo and ascertained that a check was performed to validate that the SOX settings on Bitbucket were compliant to following: • Requires >1 approver • Unapprove automatically on new changes • Changes without a pull request.	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	If the settings are not enforced, the code is rejected.	
	Attempted to deploy a change that was not compliant and ascertained that the code was rejected for deployment upon the validation check in Deployment Bamboo.	No deviation noted.
	Attempted to deploy a change that was compliant and ascertained that the code was successfully deployed upon the validation check in Deployment Bamboo.	No deviation noted.
Privileged access to Deployment Bamboo is restricted to the members of the Build Engineering team.	Inquired of the control owner and ascertained that privileged access to Deployment Bamboo was restricted to the members of the Build Engineering team.	No deviation noted.
	Inspected the list of users with privileged access to Deployment Bamboo and ascertained that access was restricted to the members of the Build Engineering team.	No deviation noted.
A Jira ticket is automatically generated if a change to the enforcement of peer review/pull requests occurs.	Inquired of the control owner and ascertained that a Jira ticket was automatically generated if a change to the enforcement of peer review or pull request occurs.	No deviation noted.
	Inspected the configuration and ascertained that a Jira ticket was automatically generated if a change to the enforcement of peer review or pull request occurs.	No deviation noted.
Atlassian uses malware protection for Windows and OSX clients. An enterprise anti-malware platform provides endpoint protection, centralized reporting and notifications.	Inquired of the control owner and ascertained that malware protection for Windows and OSX clients was implemented and security patching was enforced on Windows endpoints. Additionally, complex password on the management platform prevent Windows and OSX clients from removing or uninstalling the agent.	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
The client is installed via management platforms and protected by a complex password to prevent staff from removing or uninstalling the agent.	Inspected the configuration settings in the software used to enforce Malware protection and ascertained that malware protection was implemented and security patching was enforced on Windows endpoints.	No deviation noted.
	Attempted to uninstall the Malware protection software and ascertained that the malware protection was configured to prevent any users to uninstall the software.	No deviation noted.
IT Asset management software is used to monitor the hard drive encryption, user authentication requirements, and security patching are enforced on MacOS endpoints.	Inquired of the control owner and ascertained that IT asset management software was used for monitoring hard drive encryptions, user authentication requirements, and security patching on MacOS endpoints.	No deviation noted.
	Inspected the software used to enforce encryption and ascertained that IT Asset management software was used to monitor the hard drive encryption, user authentication requirements, and security patching was enforced on MacOS endpoints.	No deviation noted.
IT Asset management software is used to monitor hard drive encryption, user authentication requirements, and security patching on Windows endpoints.	Inquired of the control owner and ascertained that IT asset management software was used for monitoring hard drive encryptions, user authentication requirements, and security patching on Windows endpoints.	No deviation noted.
	Inspected the software used to enforce encryption and ascertained that IT Asset management software was used to monitor the hard drive encryption, user authentication requirements, and security patching was enforced on Windows endpoints.	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Users (either internal or external) may report bugs, defects, or availability, security, and confidentiality issues via https://getsupport.atlassian.com, social media, general website forms, emails, https://trust.atlassian.com, and the public bug site.	Inquired of the control owner and ascertained that customers and internal users contacted Atlassian to report issues on bugs, defects, availability, security, and confidentiality via https://getsupport.atlassian.com, social media, general website forms, emails, https://trust.atlassian.com, and the public bug site.	No deviation noted.
	Inspected the channels of reporting for issues and ascertained that customers and internal users can contact Atlassian to report issues on bugs, defects, availability, security, and confidentiality via https://getsupport.atlassian.com, social media, general website forms, emails, https://trust.atlassian.com, and the public bug site.	No deviation noted.
	Inspected a sample of issues reported by either internal or external users, and ascertained that issues were followed up and resolved per incident management process.	No deviation noted.
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.	Inquired of the control owner and ascertained that incident management process was in place, the Site Reliability ("SRE") team was responsible for incidents and problems for Atlassian services and platforms, and that incident management process met the Atlassian Incident Management Standard. Further ascertained that for incidents with severity 0 and 1, a post incident review ("PIR") and root cause analysis were performed. Further ascertained that for incidents with security level 2 and 3, a post incident review express ("PIR-X") was performed.	No deviation noted.
	Inspected a sample of incidents and issues from the incident reporting and tracking system, and ascertained that incidents and issues were monitored and resolved timely. If Jira ticket	No deviation noted.

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

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	corresponded to severity level 0 and 1, ascertained that post incident review ("PIR") and root cause analysis were performed. If a Jira ticket corresponded to severity level 2 and 3, ascertained that post incident review express ("PIR-X") was performed.	
Code scanning is performed by SourceClear on a continuous basis for Statuspage.	Inquired of the control owner and ascertained that code scanning was performed by SourceClear on a continuous basis on Statuspage's source code to identify potential vulnerabilities.	No deviation noted.
	Inspected the SourceClear configuration and ascertained that code scanning was performed by SourceClear on a continuous basis on Statuspage's source code to identify potential vulnerabilities.	No deviation noted.
	Inspected a sample of vulnerabilities identified from the code scanning through SourceClear and ascertained that vulnerabilities were reviewed by appropriate Atlassian management and tracked to completion timely.	No deviation noted.

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

CC7.0 Common Criteria Related to System Operations

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.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Code scanning is performed by SourceClear on a continuous basis for Statuspage.	Inquired of the control owner and ascertained that code scanning was performed by SourceClear on a continuous basis on Statuspage's source code to identify potential vulnerabilities.	No deviation noted.
	Inspected the SourceClear configuration and ascertained that code scanning was performed by SourceClear on a continuous basis on Statuspage's source code to identify potential vulnerabilities.	No deviation noted.
	Inspected a sample of vulnerabilities identified from the code scanning through SourceClear and ascertained that vulnerabilities were reviewed by appropriate Atlassian management and tracked to completion timely.	No deviation noted.
Penetration testing is performed by Bug Bounty on a continuous basis. Issues are reviewed and tracked to completion in a Jira ticket timely.	Inquired of the control owner and ascertained that penetration testing was performed by Bug Bounty on a continuous basis, and that issues were reviewed and tracked to completion in a Jira ticket by the Security team.	No deviation noted.
	Inspected the configuration of the BugCrowd application and observed that it ran on a continuous basis and issues were automatically created in a Jira ticket and tracked to completion by the Security team.	No deviation noted.
	Inspected a sample of issues identified from the penetration testing and ascertained that issues were reviewed and tracked to completion in a Jira ticket timely by the Security team.	No deviation noted.
Monitoring tools are in place to track and notify on the	Inquired of the control owner and ascertained that Statuspage has monitoring tools in place to track and notify on the availability of Statuspage systems and services.	No deviation noted.

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

CC7.0 Common Criteria Related to System Operations

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.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
availability of Statuspage systems and services.	Inspected the configuration of the monitoring tools in place and ascertained that monitoring tools were in place to monitor system availability of Statuspage systems and services.	No deviation noted.
	Inspected the configuration of the alert settings and ascertained that notifications were communicated to the appropriate Statuspage and Micros group.	No deviation noted.
	Inspected the resolution for a sample of HOT tickets created and ascertained that corrective actions were followed up and timely resolved.	No deviation noted.
Technical vulnerability management is implemented using vulnerability scanners. Critical threats are reviewed and resolved timely.	Inquired of the control owner and ascertained that technical vulnerability management was implemented using vulnerability scanners, and critical threats were reviewed and resolved by the security team in a timely manner.	No deviation noted.
	Inspected the configuration and tool used to monitor vulnerabilities and ascertained that technical vulnerability management was implemented using vulnerability scanners, and critical threats were reviewed and resolved timely by the security team.	No deviation noted.
	Inspected a sample of vulnerabilities identified from the vulnerability scanners and ascertained that incidents and issues were monitored and resolved timely by the security team.	No deviation noted.

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

CC7.0 Common Criteria Related to System Operations

CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Penetration testing is performed by Bug Bounty on a continuous basis. Issues are reviewed and tracked to completion in a Jira ticket timely.	Inquired of the control owner and ascertained that penetration testing was performed by Bug Bounty on a continuous basis, and that issues were reviewed and tracked to completion in a Jira ticket by the Security team.	No deviation noted.
	Inspected the configuration of the BugCrowd application and observed that it ran on a continuous basis and issues were automatically created in a Jira ticket and tracked to completion by the Security team.	No deviation noted.
	Inspected a sample of issues identified from the penetration testing and ascertained that issues were reviewed and tracked to completion in a Jira ticket timely by the Security team.	No deviation noted.
Monitoring tools are in place to track and notify on the availability of Statuspage systems and services	Inquired of the control owner and ascertained that Statuspage has monitoring tools in place to track and notify on the availability of Statuspage systems and services.	No deviation noted.
	Inspected the configuration of the monitoring tools in place and ascertained that monitoring tools were in place to monitor system availability of Statuspage systems and services.	No deviation noted.
	Inspected the configuration of the alert settings and ascertained that notifications were communicated to the appropriate Statuspage and Micros group.	No deviation noted.
	Inspected the resolution for a sample of HOT tickets created and ascertained that corrective actions were followed up and timely resolved.	No deviation noted.
Technical vulnerability management is implemented	Inquired of the control owner and ascertained that technical vulnerability management was implemented using vulnerability	No deviation noted.

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

CC7.0 Common Criteria Related to System Operations

CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
using vulnerability scanners. Critical threats are reviewed and resolved timely.	scanners, and critical threats were reviewed and resolved by the security team in a timely manner.	
	Inspected the configuration and tool used to monitor vulnerabilities and ascertained that technical vulnerability management was implemented using vulnerability scanners, and critical threats were reviewed and resolved timely by the security team.	No deviation noted.
	Inspected a sample of vulnerabilities identified from the vulnerability scanners and ascertained that incidents and issues were monitored and resolved timely by the security team.	No deviation noted.
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.	Inquired of the control owner and ascertained that incident management process was in place, the Site Reliability ("SRE") team was responsible for incidents and problems for Atlassian services and platforms, and that incident management process met the Atlassian Incident Management Standard. Further ascertained that for incidents with severity 0 and 1, a post incident review ("PIR") and root cause analysis were performed. Further ascertained that for incidents with security level 2 and 3, a post incident review express ("PIR-X") was performed.	No deviation noted.
	Inspected a sample of incidents and issues from the incident reporting and tracking system, and ascertained that incidents and issues were monitored and resolved timely. If Jira ticket corresponded to severity level 0 and 1, ascertained that post incident review ("PIR") and root cause analysis were performed. If a Jira ticket corresponded to severity level 2 and 3,	No deviation noted.

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

CC7.0 Common Criteria Related to System Operations

CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	ascertained that post incident review express ("PIR-X") was performed.	

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

CC7.0 Common Criteria Related to System Operations

CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Penetration testing is performed by Bug Bounty on a continuous basis. Issues are reviewed and tracked to completion in a Jira ticket timely.	Inquired of the control owner and ascertained that penetration testing was performed by Bug Bounty on a continuous basis, and that issues were reviewed and tracked to completion in a Jira ticket by the Security team.	No deviation noted.
	Inspected the configuration of the BugCrowd application and observed that it ran on a continuous basis and issues were automatically created in a Jira ticket and tracked to completion by the Security team.	No deviation noted.
	Inspected a sample of issues identified from the penetration testing and ascertained that issues were reviewed and tracked to completion in a Jira ticket timely by the Security team.	No deviation noted.
Technical vulnerability management is implemented using vulnerability scanners. Critical threats are reviewed and resolved timely.	Inquired of the control owner and ascertained that technical vulnerability management was implemented using vulnerability scanners, and critical threats were reviewed and resolved by the security team in a timely manner.	No deviation noted.
	Inspected the configuration and tool used to monitor vulnerabilities and ascertained that technical vulnerability management was implemented using vulnerability scanners, and critical threats were reviewed and resolved timely by the security team.	No deviation noted.
	Inspected a sample of vulnerabilities identified from the vulnerability scanners and ascertained that incidents and issues were monitored and resolved timely by the security team.	No deviation noted.
An organizational wide incident management process is in place, with the SRE team responsible	Inquired of the control owner and ascertained that incident management process was in place, the Site Reliability ("SRE") team was responsible for incidents and problems for Atlassian	No deviation noted.

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

CC7.0 Common Criteria Related to System Operations

CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
for incidents and problems for Atlassian services and platforms. Incident management process must meet the Atlassian Incident Management Standard.	services and platforms, and that incident management process met the Atlassian Incident Management Standard. Further ascertained that for incidents with severity 0 and 1, a post incident review ("PIR") and root cause analysis were performed. Further ascertained that for incidents with security level 2 and 3, a post incident review express ("PIR-X") was performed.	
	Inspected a sample of incidents and issues from the incident reporting and tracking system, and ascertained that incidents and issues were monitored and resolved timely. If Jira ticket corresponded to severity level 0 and 1, ascertained that post incident review ("PIR") and root cause analysis were performed. If a Jira ticket corresponded to severity level 2 and 3, ascertained that post incident review express ("PIR-X") was performed.	No deviation noted.

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

CC7.0 Common Criteria Related to System Operations

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.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Policies are posted and available online, assigned a policy owner, and reviewed at least annually by the designated policy owner or their delegate.	Inquired of the control owner and ascertained that policies were posted and available online, assigned a policy owner, and reviewed at least annually by the designated policy owner.	No deviation noted.
	Inspected the policies and ascertained that the policies were posted and available online, assigned a policy owner, and reviewed at least annually by the designated policy owner.	No deviation noted.
Atlassian communicates its commitment to security as a top priority for its customers via Atlassian Trust Security page.	Inquired of the control owner and ascertained that Atlassian communicated its commitment to security as a top priority for its customers on the Atlassian Trust Security page.	No deviation noted.
	Inspected the Atlassian Trust Security Page and ascertained that Atlassian communicated its commitment to security as a top priority for its customers via Atlassian Trust Security page.	No deviation noted.
Penetration testing is performed by Bug Bounty on a continuous basis. Issues are reviewed and tracked to completion in a Jira ticket timely.	Inquired of the control owner and ascertained that penetration testing was performed by Bug Bounty on a continuous basis, and that issues were reviewed and tracked to completion in a Jira ticket by the Security team.	No deviation noted.
	Inspected the configuration of the BugCrowd application and observed that it ran on a continuous basis and issues were automatically created in a Jira ticket and tracked to completion by the Security team.	No deviation noted.
	Inspected a sample of issues identified from the penetration testing and ascertained that issues were reviewed and tracked to completion in a Jira ticket timely by the Security team.	No deviation noted.
Technical vulnerability management is implemented using vulnerability scanners.	Inquired of the control owner and ascertained that technical vulnerability management was implemented using vulnerability scanners, and critical threats were reviewed and resolved by the security team in a timely manner.	No deviation noted.

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

CC7.0 Common Criteria Related to System Operations

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.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Critical threats are reviewed and resolved timely.	Inspected the configuration and tool used to monitor vulnerabilities and ascertained that technical vulnerability management was implemented using vulnerability scanners, and critical threats were reviewed and resolved timely by the security team.	No deviation noted.
	Inspected a sample of vulnerabilities identified from the vulnerability scanners and ascertained that incidents and issues were monitored and resolved timely by the security team.	No deviation noted.
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.	Inquired of the control owner and ascertained that incident management process was in place, the Site Reliability ("SRE") team was responsible for incidents and problems for Atlassian services and platforms, and that incident management process met the Atlassian Incident Management Standard. Further ascertained that for incidents with severity 0 and 1, a post incident review ("PIR") and root cause analysis were performed. Further ascertained that for incidents with security level 2 and 3, a post incident review express ("PIR-X") was performed.	No deviation noted.
	Inspected a sample of incidents and issues from the incident reporting and tracking system, and ascertained that incidents and issues were monitored and resolved timely. If Jira ticket corresponded to severity level 0 and 1, ascertained that post incident review ("PIR") and root cause analysis were performed. If a Jira ticket corresponded to severity level 2 and 3, ascertained that post incident review express ("PIR-X") was performed.	No deviation noted.
Users (either internal or external) may report bugs, defects, or	Inquired of the control owner and ascertained that customers and internal users contacted Atlassian to report issues on bugs,	No deviation noted.

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

CC7.0 Common Criteria Related to System Operations

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.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
availability, security, and confidentiality issues via https://getsupport.atlassian.com, social media, general website forms, emails, https://trust.atlassian.com, and the public bug site.	defects, availability, security, and confidentiality via https://getsupport.atlassian.com, social media, general website forms, emails, https://trust.atlassian.com, and the public bug site.	
	Inspected the channels of reporting for issues and ascertained that customers and internal users can contact Atlassian to report issues on bugs, defects, availability, security, and confidentiality via https://getsupport.atlassian.com, social media, general website forms, emails, https://trust.atlassian.com, and the public bug site.	No deviation noted.
	Inspected a sample of issues reported by either internal or external users, and ascertained that issues were followed up and resolved per incident management process.	No deviation noted.
A disaster recovery policy is in place and is reviewed on an annual basis by the disaster recovery steering committee.	Inquired of the control owner and ascertained a disaster recovery policy was in place and was reviewed on an annual basis by the disaster recovery steering committee.	No deviation noted.
	Inspected and observed the disaster recovery policy, and ascertained that disaster recovery policy was in place and reviewed on an annual basis by the disaster recovery steering committee.	No deviation noted.
A disaster recovery plan is in place for Statuspage and its services which is tested on a quarterly basis. Key stakeholders are involved in the planning,	Inquired of the control owner and ascertained the disaster recovery testing was in place for Statuspage and its services, and was tested on a quarterly basis. Further ascertained that key stakeholders were involved in the planning, impact analysis, execution, and remediation (if required) in a timely manner.	No deviation noted.

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

CC7.0 Common Criteria Related to System Operations

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.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
impact analysis, execution, and remediation (if required).	Inspected the disaster recovery plan and ascertained that it was reviewed, updated, and tested quarterly, and key stakeholders were involved in the planning, impact analysis, execution, and remediation if required.	No deviation noted.
	Inspected the quarterly disaster recovery testing and ascertained that testing was performed timely, and key stakeholders were involved in the planning, impact analysis, execution, and remediation.	No deviation noted.
Statuspage data is stored in Postgres RDS instances which are automatically backed up daily by AWS. On a semi-annual basis, restoration testing is performed by the Statuspage SRE team to ensure recoverability of backups.	Inquired of the control owner and ascertained that Statuspage data was stored in Postgres RDS instances which were automatically backed up daily by AWS. Further ascertained that restoration testing was tested on a semi-annual basis by the Statuspage Site Reliability Engineering ("SRE") team to ensure recoverability of backups.	No deviation noted.
	Inspected the replication and backup configuration, and ascertained that AWS was configured to perform automatic backups on a daily basis.	No deviation noted.
	Inspected a sample of semi-annual restoration testing and ascertained that restore testing was performed successfully. Further ascertained that any issues identified from the restoration testing were investigated and resolved timely.	No deviation noted.
Replication and backups are in place to provide data redundancy and availability for Micros.	Inquired of the control owner and ascertained that replication and backups were in place to provide data redundancy and availability for Micros.	No deviation noted.
	Inspected the replication configuration and ascertained that the replications were configured real time from the primary site to a secondary site.	No deviation noted.

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

CC7.0 Common Criteria Related to System Operations

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.		
Controls Specified by Atlassian	Tests Performed by EY	Results of Tests
	Inspected a sample of replication and backups and ascertained that replications were configured real time from the primary site to a secondary site.	No deviation noted.

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

CC7.0 Common Criteria Related to System Operations

CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Atlassian communicates its commitment to security as a top priority for its customers via Atlassian Trust Security page.	Inquired of the control owner and ascertained that Atlassian communicated its commitment to security as a top priority for its customers on the Atlassian Trust Security page.	No deviation noted.
	Inspected the Atlassian Trust Security Page and ascertained that Atlassian communicated its commitment to security as a top priority for its customers via Atlassian Trust Security page.	No deviation noted.
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.	Inquired of the control owner and ascertained that incident management process was in place, the Site Reliability ("SRE") team was responsible for incidents and problems for Atlassian services and platforms, and that incident management process met the Atlassian Incident Management Standard. Further ascertained that for incidents with severity 0 and 1, a post incident review ("PIR") and root cause analysis were performed. Further ascertained that for incidents with security level 2 and 3, a post incident review express ("PIR-X") was performed.	No deviation noted.
	Inspected a sample of incidents and issues from the incident reporting and tracking system, and ascertained that incidents and issues were monitored and resolved timely. If Jira ticket corresponded to severity level 0 and 1, ascertained that post incident review ("PIR") and root cause analysis were performed. If a Jira ticket corresponded to severity level 2 and 3, ascertained that post incident review express ("PIR-X") was performed.	No deviation noted.
Users (either internal or external) may report bugs, defects, or availability, security, and confidentiality issues via	Inquired of the control owner and ascertained that customers and internal users contacted Atlassian to report issues on bugs, defects, availability, security, and confidentiality via https://getsupport.atlassian.com, social media, general website	No deviation noted.

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

CC7.0 Common Criteria Related to System Operations

CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
https://getsupport.atlassian.com, social media, general website forms, emails, https://trust.atlassian.com, and the public bug site.	forms, emails, https://trust.atlassian.com, and the public bug site.	
	Inspected the channels of reporting for issues and ascertained that customers and internal users can contact Atlassian to report issues on bugs, defects, availability, security, and confidentiality via https://getsupport.atlassian.com, social media, general website forms, emails, https://trust.atlassian.com, and the public bug site.	No deviation noted.
	Inspected a sample of issues reported by either internal or external users, and ascertained that issues were followed up and resolved per incident management process.	No deviation noted.
A disaster recovery policy is in place and is reviewed on an annual basis by the disaster recovery steering committee.	Inquired of the control owner and ascertained a disaster recovery policy was in place and was reviewed on an annual basis by the disaster recovery steering committee.	No deviation noted.
	Inspected and observed the disaster recovery policy, and ascertained that disaster recovery policy was in place and reviewed on an annual basis by the disaster recovery steering committee.	No deviation noted.
A disaster recovery plan is in place for Statuspage and its services which is tested on a quarterly basis. Key stakeholders are involved in the planning, impact analysis, execution, and remediation (if required).	Inquired of the control owner and ascertained the disaster recovery testing was in place for Statuspage and its services, and was tested on a quarterly basis. Further ascertained that key stakeholders were involved in the planning, impact analysis, execution, and remediation (if required) in a timely manner.	No deviation noted.
	Inspected the disaster recovery plan and ascertained that it was reviewed, updated, and tested quarterly, and key stakeholders were involved in the planning, impact analysis, execution, and remediation if required.	No deviation noted.

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

CC7.0 Common Criteria Related to System Operations

CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	Inspected the quarterly disaster recovery testing and ascertained that testing was performed timely, and key stakeholders were involved in the planning, impact analysis, execution, and remediation.	No deviation noted.
Statuspage data is stored in Postgres RDS instances which are automatically backed up daily by AWS. On a semi-annual basis, restoration testing is performed by the Statuspage SRE team to ensure recoverability of backups.	Inquired of the control owner and ascertained that Statuspage data was stored in Postgres RDS instances which were automatically backed up daily by AWS. Further ascertained that restoration testing was tested on a semi-annual basis by the Statuspage Site Reliability Engineering ("SRE") team to ensure recoverability of backups.	No deviation noted.
	Inspected the replication and backup configuration, and ascertained that AWS was configured to perform automatic backups on a daily basis.	No deviation noted.
	Inspected a sample of semi-annual restoration testing and ascertained that restore testing was performed successfully. Further ascertained that any issues identified from the restoration testing were investigated and resolved timely.	No deviation noted.
Replication and backups are in place to provide data redundancy and availability for Micros.	Inquired of the control owner and ascertained that replication and backups were in place to provide data redundancy and availability for Micros.	No deviation noted.
	Inspected the replication configuration and ascertained that the replications were configured real time from the primary site to a secondary site.	No deviation noted.
	Inspected a sample of replication and backups and ascertained that replications were configured real time from the primary site to a secondary site.	No deviation noted.

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

CC8.0 Common Criteria Related to Change Management

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.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
The Micros platform will not allow code artefacts to deploy or run on the platform unless they have been peer reviewed and have passed green build testing.	Inquired of the control owner and ascertained that changes were documented through pull requests, and peer review and passed green build testing was required prior to merging the code to the master branch.	No deviation noted.
	Inspected the Bitbucket configuration and ascertained that changes were documented through pull requests, and that the Bitbucket repositories would not allow changes to deploy or run on the platform unless they have been peer reviewed and have passed green build testing.	No deviation noted.
	Inspected a sample of merged pull requests and ascertained that documented peer review and green build testing was required prior to merging the code to master branch.	No deviation noted.
Micros will only pull deployment artefacts from the restricted namespace. Only deployment-bamboo has the credentials to push to the restricted namespace.	Inquired of the control owner and ascertained that artefacts with peer review and passed green build testing were deployed from a restricted namespace by deployment-bamboo bot account.	No deviation noted.
	Inspected the list of accounts with ability to commit changes to Docker and ascertained that only deployment-bamboo was assigned to push changes to Docker.	No deviation noted.
	Attempted to push a change to the restricted Docker namespace using an end user account and ascertained that the deployed change was denied.	No deviation noted.
Bitbucket does not allow a pull request to be approved by the same user who requests it.	Inquired of the control owner and ascertained that Bitbucket does not allow a pull requests to be approved by the same user who requests it.	No deviation noted.
	Attempted a creation of pull request and ascertained that Bitbucket did not allow a pull request to be approved by the same user who requested it.	No deviation noted.

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

CC8.0 Common Criteria Related to Change Management

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.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	Inspected a sample of merged pull requests and ascertained that the peer reviewer requester was not the same as the approver.	No deviation noted.
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.	Inquired of the control owner and ascertained that Bamboo would not allow code to be deployed unless it has passed green build testing.	No deviation noted.
	Attempted to deploy a red build code and ascertained that it did not allow the code to be deployed unless it has passed green build testing.	No deviation noted.
	Attempted to deploy a green build code and ascertained that Bamboo allowed the code to be deployed.	No deviation noted.
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 were not enforced, the code is rejected.	Inquired of the control owner and ascertained that 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.	No deviation noted.
	Inspected the API configuration in Deployment bamboo and ascertained that a check was performed to validate that the SOX settings on Bitbucket were compliant to following: • Requires >1 approver • Unapprove automatically on new changes • Changes without a pull request.	No deviation noted.

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

CC8.0 Common Criteria Related to Change Management

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.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	If the settings are not enforced, the code is rejected.	
	Attempted to deploy a change that was not compliant and ascertained that the code was rejected for deployment upon the validation check in Deployment Bamboo.	No deviation noted.
	Attempted to deploy a change that was compliant and ascertained that the code was successfully deployed upon the validation check in Deployment Bamboo.	No deviation noted.
Privileged access to Deployment Bamboo is restricted to the members of the Build Engineering team.	Inquired of the control owner and ascertained that privileged access to Deployment Bamboo was restricted to the members of the Build Engineering team.	No deviation noted.
	Inspected the list of users with privileged access to Deployment Bamboo and ascertained that access was restricted to the members of the Build Engineering team.	No deviation noted.
A Jira ticket is automatically generated if a change to the enforcement of peer review/pull requests occurs.	Inquired of the control owner and ascertained that a Jira ticket was automatically generated if a change to the enforcement of peer review or pull request occurs.	No deviation noted.
	Inspected the configuration and ascertained that a Jira ticket was automatically generated if a change to the enforcement of peer review or pull request occurs.	No deviation noted.

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

CC9.0 Common Criteria Related to Risk Mitigation

CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Atlassian has defined an ERM process and conducts an enterprise risk assessment on an annual basis, which includes key product stakeholders.	Inquired of the control owner and ascertained that Atlassian had defined a risk management process, and conducted an enterprise risk assessment on an annual basis, inclusive of key product stakeholders.	No deviation noted.
	Inspected the ERM assessment and ascertained that Atlassian had defined an ERM process, and the enterprise risk assessment was performed on an annual basis, which includes key product stakeholders. Additionally, a monthly meeting was held to discuss updates to the enterprise risk assessment and results.	No deviation noted.
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.	Inquired of the control owner and ascertained that the Atlassian Risk and Compliance team evaluated the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Atlassian maintained a risk and controls matrix within their GRC tool.	No deviation noted.
	Inspected the GRC Tool used by Atlassian and ascertained that the Atlassian Risk and Compliance team evaluated the design of controls and mitigation strategies at least annually, including identifying risks and recommending changes in the control environment. Further ascertained that Atlassian maintained a risk and controls matrix within their GRC tool.	No deviation noted.
A disaster recovery policy is in place and is reviewed on an annual basis by the disaster recovery steering committee.	Inquired of the control owner and ascertained a disaster recovery policy was in place and was reviewed on an annual basis by the disaster recovery steering committee.	No deviation noted.
	Inspected and observed the disaster recovery policy, and ascertained that disaster recovery policy was in place and reviewed on an annual basis by the disaster recovery steering committee.	No deviation noted.

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

CC9.0 Common Criteria Related to Risk Mitigation

CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
A disaster recovery plan is in place for Statuspage and its services which is tested on a quarterly basis. Key stakeholders are involved in the planning, impact analysis, execution, and remediation (if required).	Inquired of the control owner and ascertained the disaster recovery testing was in place for Statuspage and its services, and was tested on a quarterly basis. Further ascertained that key stakeholders were involved in the planning, impact analysis, execution, and remediation (if required) in a timely manner.	No deviation noted.
	Inspected the disaster recovery plan and ascertained that it was reviewed, updated, and tested quarterly, and key stakeholders were involved in the planning, impact analysis, execution, and remediation if required.	No deviation noted.
	Inspected the quarterly disaster recovery testing and ascertained that testing was performed timely, and key stakeholders were involved in the planning, impact analysis, execution, and remediation.	No deviation noted.
Replication and backups are in place to provide data redundancy and availability for Micros.	Inquired of the control owner and ascertained that replication and backups were in place to provide data redundancy and availability for Micros.	No deviation noted.
	Inspected the replication configuration and ascertained that the replications were configured real time from the primary site to a secondary site.	No deviation noted.
	Inspected a sample of replication and backups and ascertained that replications were configured real time from the primary site to a secondary site.	No deviation noted.

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

CC9.0 Common Criteria Related to Risk Mitigation

CC9.2 The entity assesses and manages risks associated with vendors and business partners.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Vendor agreements, including any security, availability and confidentiality commitments, are reviewed during the procurement process.	Inquired of the control owner and ascertained that vendor agreements, including any security, availability, and confidentiality commitments, were reviewed during the procurement process.	No deviation noted.
	Inspected a sample of new vendors' third-party contracts and ascertained that the contracts included security, availability, and confidentiality commitments, and the contracts were executed between the third-party and Atlassian during the procurement process.	No deviation noted.
Atlassian reviews the SOC reports of the vendors on an annual basis.	Inquired of the control owner and ascertained that Atlassian reviewed the SOC reports of the vendors ("subservice organizations") on an annual basis.	No deviation noted.
	Inspected the Jira ticket for the review of the SOC 2 or equivalent attestation reports and ascertained that leadership reviewed the reports annually. Reviews included an assessment of complementary user entity controls, subservice organizations, and mapping of the controls to key risks. If there were exceptions, Atlassian reviewed the severity and impact of the exceptions, and if needed, followed-up with the individual vendor.	No deviation noted.

Additional Criteria for Availability

A1.0 Additional Criteria to Availability Criteria

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.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Statuspage performs quarterly system-wide capacity audits to monitor utilization levels and adjust accordingly.	Inquired of the control owner and ascertained that system-wide capacity audits to monitor utilization levels were performed for Statuspage on a quarterly basis, and adjustments were made if necessary.	No deviation noted.
	Inspected a sample of quarterly review of the capacity audit results and ascertained that system-wide capacity reviews to monitor utilization levels were performed for Statuspage on a quarterly basis, and adjustments were made if necessary.	No deviation noted.
Availability is published so that Customers may check the status/uptime of Statuspage.	Inquired of the control owner and ascertained that availability was published in the customer-facing website so that customers could check the status and uptime of Statuspage.	No deviation noted.
	Inspected the customer-facing website and ascertained that availability was published real-time, and the status and uptime metrics of Statuspage were communicated to customers.	No deviation noted.
Monitoring tools are in place to track and notify on the availability of Statuspage systems and services.	Inquired of the control owner and ascertained that Statuspage has monitoring tools in place to track and notify on the availability of Statuspage systems and services.	No deviation noted.
	Inspected the configuration of the monitoring tools in place and ascertained that monitoring tools were in place to monitor system availability of Statuspage systems and services.	No deviation noted.
	Inspected the configuration of the alert settings and ascertained that notifications were communicated to the appropriate Statuspage and Micros group.	No deviation noted.
	Inspected the resolution for a sample of HOT tickets created and ascertained that corrective actions were followed up and timely resolved.	No deviation noted.

Additional Criteria for Availability

A1.0 Additional Criteria to Availability Criteria

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.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Replication and backups are in place to provide data redundancy and availability for Micros.	Inquired of the control owner and ascertained that replication and backups were in place to provide data redundancy and availability for Micros.	No deviation noted.
	Inspected the replication configuration and ascertained that the replications were configured real time from the primary site to a secondary site.	No deviation noted.
	Inspected a sample of replication and backups and ascertained that replications were configured real time from the primary site to a secondary site.	No deviation noted.
Statuspage data is stored in Postgres RDS instances which are automatically backed up daily by AWS. On a semi-annual basis, restoration testing is performed by the Statuspage SRE team to ensure recoverability of backups.	Inquired of the control owner and ascertained that Statuspage data was stored in Postgres RDS instances which were automatically backed up daily by AWS. Further ascertained that restoration testing was tested on a semi-annual basis by the Statuspage Site Reliability Engineering ("SRE") team to ensure recoverability of backups.	No deviation noted.
	Inspected the replication and backup configuration, and ascertained that AWS was configured to perform automatic backups on a daily basis.	No deviation noted.
	Inspected a sample of semi-annual restoration testing and ascertained that restore testing was performed successfully. Further ascertained that any issues identified from the restoration testing were investigated and resolved timely.	No deviation noted.
A disaster recovery policy is in place and is reviewed on an	Inquired of the control owner and ascertained a disaster recovery policy was in place and was reviewed on an annual basis by the disaster recovery steering committee.	No deviation noted.

Additional Criteria for Availability

A1.0 Additional Criteria to Availability Criteria

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.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
annual basis by the disaster recovery steering committee.	Inspected and observed the disaster recovery policy, and ascertained that disaster recovery policy was in place and reviewed on an annual basis by the disaster recovery steering committee.	No deviation noted.
A disaster recovery plan is in place for Statuspage and its services which is tested on a quarterly basis. Key stakeholders are involved in the planning, impact analysis, execution, and remediation (if required).	Inquired of the control owner and ascertained the disaster recovery testing was in place for Statuspage and its services, and was tested on a quarterly basis. Further ascertained that key stakeholders were involved in the planning, impact analysis, execution, and remediation (if required) in a timely manner.	No deviation noted.
	Inspected the disaster recovery plan and ascertained that it was reviewed, updated, and tested quarterly, and key stakeholders were involved in the planning, impact analysis, execution, and remediation if required.	No deviation noted.
	Inspected the quarterly disaster recovery testing and ascertained that testing was performed timely, and key stakeholders were involved in the planning, impact analysis, execution, and remediation.	No deviation noted.
Atlassian reviews the SOC reports of the vendors on an annual basis.	Inquired of the control owner and ascertained that Atlassian reviewed the SOC reports of the vendors ("subservice organizations") on an annual basis.	No deviation noted.
	Inspected the Jira ticket for the review of the SOC 2 or equivalent attestation reports and ascertained that leadership reviewed the reports annually. Reviews included an assessment of complementary user entity controls, subservice organizations, and mapping of the controls to key risks. If there were exceptions, Atlassian reviewed the severity and impact of	No deviation noted.

Additional Criteria for Availability

A1.0 Additional Criteria to Availability Criteria

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.		
Controls Specified by Atlassian	Tests Performed by EY	Results of Tests
	the exceptions, and if needed, followed-up with the individual vendor.	

Additional Criteria for Availability

A1.0 Additional Criteria to Availability Criteria

A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Replication and backups are in place to provide data redundancy and availability for Micros.	Inquired of the control owner and ascertained that replication and backups were in place to provide data redundancy and availability for Micros.	No deviation noted.
	Inspected the replication configuration and ascertained that the replications were configured real time from the primary site to a secondary site.	No deviation noted.
	Inspected a sample of replication and backups and ascertained that replications were configured real time from the primary site to a secondary site.	No deviation noted.
Statuspage data is stored in Postgres RDS instances which are automatically backed up daily by AWS. On a semi-annual basis, restoration testing is performed by the Statuspage SRE team to ensure recoverability of backups.	Inquired of the control owner and ascertained that Statuspage data was stored in Postgres RDS instances which were automatically backed up daily by AWS. Further ascertained that restoration testing was tested on a semi-annual basis by the Statuspage Site Reliability Engineering ("SRE") team to ensure recoverability of backups.	No deviation noted.
	Inspected the replication and backup configuration, and ascertained that AWS was configured to perform automatic backups on a daily basis.	No deviation noted.
	Inspected a sample of semi-annual restoration testing and ascertained that restore testing was performed successfully. Further ascertained that any issues identified from the restoration testing were investigated and resolved timely.	No deviation noted.
A disaster recovery policy is in place and is reviewed on an	Inquired of the control owner and ascertained a disaster recovery policy was in place and was reviewed on an annual basis by the disaster recovery steering committee.	No deviation noted.

Additional Criteria for Availability

A1.0 Additional Criteria to Availability Criteria

A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
annual basis by the disaster recovery steering committee.	Inspected and observed the disaster recovery policy, and ascertained that disaster recovery policy was in place and reviewed on an annual basis by the disaster recovery steering committee.	No deviation noted.

Additional Criteria for Confidentiality

C1.0 Additional Criteria to Confidentiality Criteria

C1.1 The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Data is classified according to company policy.	Inquired of the control owner and ascertained data was classified according to company policy.	No deviation noted.
	Inspected the company policy and ascertained that data classification level was documented within the policy.	No deviation noted.
	Inspected a sample of each data classification type and ascertained that it was assigned a classification level according to Atlassian's Data Security and Information Lifecycle Management Policy.	No deviation noted.
Production data is not used in non-production environments and must be protected in alignment with Atlassian's System Acquisition, Development, and Maintenance Policy.	Inquired of the control owner and ascertained that production data was not used in non-production environments, and must be protected in alignment with Atlassian's System Acquisition, Development, and Maintenance Policy.	No deviation noted.
	Inspected a customer's production data in the non-production environment and ascertained that the customer's production data did not exist in the non-production environment.	No deviation noted.
Statuspage data is encrypted at rest.	Inquired of the control owner and ascertained that Statuspage data was encrypted at rest.	No deviation noted.
	Inspected the AWS encryption configuration and ascertained that Statuspage data was encrypted at rest.	No deviation noted.
External users securely connect to Statuspage via the encrypted SSL protocol.	Inquired of the control owner and ascertained the external users were connected to Statuspage using encrypted traffic via SSL protocol.	No deviation noted.
	Inspected the Statuspage webpage and ascertained the external users were connected to Statuspage using encrypted traffic via SSL protocol.	No deviation noted.
Atlassian reviews the SOC reports of the vendors on an annual basis.	Inquired of the control owner and ascertained that Atlassian reviewed the SOC reports of the vendors ("subservice organizations") on an annual basis.	No deviation noted.

Additional Criteria for Confidentiality

C1.0 Additional Criteria to Confidentiality Criteria

C1.1 The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	Inspected the Jira ticket for the review of the SOC 2 or equivalent attestation reports and ascertained that leadership reviewed the reports annually. Reviews included an assessment of complementary user entity controls, subservice organizations, and mapping of the controls to key risks. If there were exceptions, Atlassian reviewed the severity and impact of the exceptions, and if needed, followed-up with the individual vendor.	No deviation noted.
Statuspage assigns unique identifiers upon creation to customer data.	Inquired of the control owner and ascertained that Statuspage assigned unique identifiers upon creation of customer data.	No deviation noted.
	Inspected the Statuspage configuration and ascertained that all customers and users were configured to be provisioned with unique identifiers in Statuspage.	No deviation noted.
	Inspected a customer account and ascertained that a unique ID was assigned to the customer in the Statuspage production database.	No deviation noted.
Statuspage data is deleted within 30 days of receipt of a request for deletion.	Inquired of the control owner and ascertained that Statuspage data was deleted within 30 days of receipt of a request for deletion.	No deviation noted.
	Inspected the Statuspage database for a sample of customers and ascertained that Statuspage data was deleted within 30 days of receipt of a request for deletion.	No deviation noted.
Vendor agreements, including any security, availability and confidentiality commitments, are	Inquired of the control owner and ascertained that vendor agreements, including any security, availability, and confidentiality commitments, were reviewed during the procurement process.	

Additional Criteria for Confidentiality

C1.0 Additional Criteria to Confidentiality Criteria

C1.1 The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
reviewed during the procurement process.	Inspected a sample of new vendors' third-party contracts and ascertained that the contracts included security, availability, and confidentiality commitments, and the contracts were executed between the third-party and Atlassian during the procurement process.	
Privileged access of Atlassian users to EC2 production environment is restricted to authorized and appropriate users only.	Inquired of the control owner and ascertained privileged access of Atlassian users to EC2 production environment was restricted to authorized and appropriate users only.	No deviation noted.
	Inspected the complete list of users with privileged access to EC2 production environment and ascertained that access was restricted to authorized and appropriate users only.	No deviation noted.

Additional Criteria for Confidentiality

C1.0 Additional Criteria to Confidentiality Criteria

C1.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
Data is classified according to company policy.	Inquired of the control owner and ascertained data was classified according to company policy.	No deviation noted.
	Inspected the company policy and ascertained that data classification level was documented within the policy.	No deviation noted.
	Inspected a sample of each data classification type and ascertained that it was assigned a classification level according to Atlassian's Data Security and Information Lifecycle Management Policy.	No deviation noted.
Statuspage data is deleted within 30 days of receipt of a request for deletion.	Inquired of the control owner and ascertained that Statuspage data was deleted within 30 days of receipt of a request for deletion.	No deviation noted.
	Inspected the Statuspage database for a sample of customers and ascertained that Statuspage data was deleted within 30 days of receipt of a request for deletion.	No deviation noted.
Vendor agreements, including any security, availability and confidentiality commitments, are reviewed during the procurement process.	Inquired of the control owner and ascertained that vendor agreements, including any security, availability, and confidentiality commitments, were reviewed during the procurement process.	No deviation noted.
	Inspected a sample of new vendors' third-party contracts and ascertained that the contracts included security, availability, and confidentiality commitments, and the contracts were executed between the third-party and Atlassian during the procurement process.	No deviation noted.
Atlassian reviews the SOC reports of the vendors on an annual basis.	Inquired of the control owner and ascertained that Atlassian reviewed the SOC reports of the vendors ("subservice organizations") on an annual basis.	No deviation noted.

Additional Criteria for Confidentiality

C1.0 Additional Criteria to Confidentiality Criteria

C1.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality.		
Controls Specified by Atlassian	**Tests Performed by EY**	**Results of Tests**
	Inspected the Jira ticket for the review of the SOC 2 or equivalent attestation reports and ascertained that leadership reviewed the reports annually. Reviews included an assessment of complementary user entity controls, subservice organizations, and mapping of the controls to key risks. If there were exceptions, Atlassian reviewed the severity and impact of the exceptions, and if needed, followed-up with the individual vendor.	No deviation noted.