



Microsoft Corporation - Azure DevOps

System and Organization Controls (SOC) 2 Report

October 1, 2022 to September 30, 2023

Table of contents

Executive Summary	1
Section I: Independent Service Auditor's Report for the Security, Availability, Processing Integrity, and Confidentiality Criteria, and C5	3
Section II: Management of Microsoft's Assertion	8
Section III: Management of Microsoft's Description of its Azure DevOps System	11
Section IV: Management of Microsoft's Description of its Relevant Criteria and Objectives and Related Controls, and Independent Service Auditor's Description of Tests of Controls and Results	43
Section V: Other Information Provided by Management of Microsoft	199

Executive Summary

Microsoft Azure DevOps

Scope	Microsoft Azure DevOps
Period of Examination	October 1, 2022 to September 30, 2023
Applicable Trust Services Criteria	Security, Availability, Processing Integrity, and Confidentiality
Additional Criteria	Bundesamt für Sicherheit in der Informationstechnik Cloud Computing Compliance Criteria Catalogue (C5)
Subservice Provider	Microsoft Azure
Opinion Result	Unqualified
Testing Exceptions	0

Section I: Independent Service Auditor's Report for the Security, Availability, Processing Integrity, and Confidentiality Criteria, and C5

Section I: Independent Service Auditor's Report for the Security, Availability, Processing Integrity, and Confidentiality Criteria, and C5

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Scope

We have examined the description of the Azure DevOps¹ system of management of Microsoft Corporation (the "Service Organization" or "Microsoft") included in Section III, "Management of Microsoft's Description of its Azure DevOps System" throughout the period October 1, 2022 to September 30, 2023 (the "Description") based on the criteria for a Description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*, in *AICPA Description Criteria*, ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the Description throughout the period October 1, 2022 to September 30, 2023, to provide reasonable assurance that Microsoft's service commitments and system requirements would be achieved based on the trust services criteria relevant to security, availability, processing integrity, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in *AICPA Trust Services Criteria*. We have also examined the suitability of the design and operating effectiveness of the controls to meet the objectives set forth in the Bundesamt für Sicherheit in der Informationstechnik (BSI) Cloud Computing Compliance Criteria Catalogue ("C5"). BSI requires an attestation in order for the service provider to be considered certified as having met the objectives set forth in the BSI's C5.

The information included in Section V, "Other Information Provided by Management of Microsoft" is presented by management of Microsoft to provide additional information and is not a part of management of Microsoft's Description of its Azure DevOps system made available to user entities during the period October 1, 2022 to September 30, 2023. Information in Section V has not been subjected to the procedures applied in the examination of the Description of the Azure DevOps system and of the suitability of the design and operating effectiveness of controls, to achieve Microsoft's service commitments and system requirements based on the applicable trust services criteria and the objectives set forth in C5, and, accordingly, we express no opinion on it.

Microsoft uses Microsoft Azure ("Azure") as a cloud platform and datacenter service to host its services ("subservice organization"). The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Microsoft, to achieve Microsoft's service commitments and system requirements based on the applicable trust services criteria and the objectives set forth in C5. The Description presents Microsoft's controls, the applicable trust services criteria, the objectives set forth in C5 and the types of complementary subservice organization controls assumed in the design of Microsoft's controls. The Description does not disclose the actual controls at the subservice

¹ Azure DevOps comprises of in-scope features defined in the *Report Scope and Boundary* subsection in Section III of this SOC 2 report.

organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The Description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Microsoft, to achieve Microsoft's service commitments and system requirements based on the applicable trust services criteria and the objectives set forth in C5. The Description presents Microsoft's controls, the applicable trust services criteria, the objectives set forth in C5, and the complementary user entity controls assumed in the design of Microsoft's controls. 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 complimentary user entity controls.

Service Organization's Responsibilities

Management of Microsoft 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 Microsoft's service commitments and system requirements would be achieved. Management of Microsoft has provided the accompanying assertion in Section II titled "Management of Microsoft's Assertion" (the "Assertion") about the Description and the suitability of the design and operating effectiveness of controls stated therein. Management of Microsoft is also responsible for preparing the Description and Assertion, including the completeness, accuracy, and method of presentation of the Description and Assertion; providing the services covered by the Description; selecting the applicable trust services criteria and stating the related controls in the Description; and identifying the risks that threaten the achievement of the Service Organization's service commitments and system requirements and the objectives set forth in C5.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the Description and on the suitability of design and operating effectiveness of the controls stated in the Description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and International Standard on Assurance Engagements (ISAE) 3000 (Revised), *Assurance Engagements Other Than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board (IAASB). Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, the Description is presented in accordance with the description criteria, and the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the Microsoft's service commitments and system requirements would be achieved based on the applicable trust services criteria and the objectives set forth in C5 were achieved. We believe that the evidence we 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.
- Assessing the risks that the Description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the Description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the Description were suitably designed to provide reasonable assurance that the Service Organization would achieve its service

commitments and system requirements based on the applicable trust services criteria and the objectives set forth in C5.

- Testing the operating effectiveness of those controls stated in the Description to provide reasonable assurance that Microsoft achieved its service commitments and system requirements based on the applicable trust services criteria and the objectives set forth in C5.
- Evaluating the overall presentation of the Description.

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

Service Auditor's Independence and Quality Control

We are required to be independent and to meet our other ethical responsibilities in accordance with the Code of Professional Conduct established by the AICPA and the International Ethics Standards Board for Accountants' Code of Ethics for Professional Accountants. We have complied with those requirements. We applied the Statements on Quality Control Standards established by the AICPA and the International Standards on Quality Management issued by the IAASB and, accordingly, maintain a comprehensive system of quality control.

Inherent Limitations

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

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

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria and the objectives set forth in C5 are achieved. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls tested, and the nature, timing, and results of those tests are listed in Section IV, "Management of Microsoft's Description of its Relevant Criteria and Objectives and Related Controls, and Independent Service Auditor's Description of Tests of Controls and Results."

Opinion

In our opinion, in all material respects:

- a. The Description presents Microsoft's Azure DevOps system that was designed and implemented throughout the period October 1, 2022 to September 30, 2023 in accordance with the description criteria.
- b. The controls stated in the Description were suitably designed throughout the period October 1, 2022 to September 30, 2023 to provide reasonable assurance that Microsoft's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and the subservice organization and user entities applied the complementary controls assumed in the design of Microsoft's controls throughout that period.

- c. The controls stated in the Description operated effectively throughout the period October 1, 2022 to September 30, 2023, to provide reasonable assurance that Microsoft's service commitments and system requirements would be achieved based on the applicable trust services criteria, if subservice organization controls and user entities applied the complementary controls assumed in the design of Microsoft's controls operated effectively throughout that period.
- d. The controls stated in the description were implemented and operated effectively to meet the requirements set forth in the objectives set forth in the BSI C5, if subservice organization controls and user entities applied the complementary controls assumed in the design of Microsoft's controls operated effectively throughout the period October 1, 2022 to September 30, 2023.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of management of Microsoft, user entities of the Microsoft's Azure DevOps system during some or all of the period October 1, 2022 to September 30, 2023, business partners of Microsoft subject to risks arising from interactions with the Microsoft's system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by Microsoft.
- How the Microsoft's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and complementary subservice organization controls and how they interact with related controls at Microsoft to achieve the Microsoft's commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the Microsoft's services.
- The applicable trust services criteria and the objectives set forth in C5.
- The risks that may threaten the achievement of the Microsoft'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.

Deloitte & Touche LLP

November 15, 2023

Section II: Management of Microsoft's Assertion



Section II: Management of Microsoft's Assertion

We have prepared the description of the Azure DevOps² system of management of Microsoft Corporation (the "Service Organization" or "Microsoft") included in section III, "Management of Microsoft's Description of its Azure DevOps System" throughout the period October 1, 2022 to September 30, 2023 (the "Description") based on criteria for a description of a service organization's system in DC Section 200, 2018 *Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*, in AICPA *Description Criteria*, ("description criteria"). The Description is intended to provide users with information about our system that may be useful when assessing the risks arising from interactions with Microsoft's system, particularly information about system controls that Microsoft has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, and confidentiality ("applicable trust services criteria") set forth in TSP Section 100, 2017 *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria* and the objectives set forth in the Bundesamt für Sicherheit in der Informationstechnik (BSI) Cloud Computing Compliance Criteria Catalogue ("C5") were achieved.

Microsoft uses Microsoft Azure ("Azure") for platform and data center services. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Microsoft, to achieve Microsoft's service commitments and system requirements based on the applicable trust services criteria and the objectives set forth in C5. The Description presents Microsoft's controls, the applicable trust services criteria, the objectives set forth in C5, and the types of complementary subservice organization controls assumed in the design of Microsoft's controls. The Description does not disclose the actual controls at the subservice organization. The Description does not extend to controls of the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Microsoft, to achieve Microsoft's service commitments and system requirements based on the applicable trust services criteria and the objectives set forth in C5. The Description presents Microsoft's controls, the applicable trust services criteria, the objectives set forth in C5, and the complementary user entity controls assumed in the design of Microsoft's controls. The Description does not extend to controls of the user entities.

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

- a. The Description presents Microsoft's system that was designed and implemented throughout the period October 1, 2022 to September 30, 2023 in accordance with the description criteria.
- b. The controls stated in the Description were suitably designed throughout the period October 1, 2022 to September 30, 2023, to provide reasonable assurance that Microsoft's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of Microsoft's controls throughout that period.
- c. The controls stated in the Description operated effectively throughout the period October 1, 2022 to September 30, 2023, to provide reasonable assurance that Microsoft's service commitments and system

² Azure DevOps comprises of in-scope features defined in the *Report Scope and Boundary* subsection in Section III of this SOC 2 report.

requirements were achieved based on the applicable trust services criteria, if the subservice organization and user entities applied the complementary controls assumed in the design of Microsoft's controls operated effectively throughout that period.

- d. The controls stated in the description were implemented and operated effectively to meet the requirements set forth in the objectives set forth in the BSI C5, if subservice organization controls and user entities applied the complementary controls assumed in the design of Microsoft's controls operated effectively throughout the period October 1, 2022 to September 30, 2023.

Section III:

Management of Microsoft's

Description of its Azure DevOps

System

Section III: Management of Microsoft's Description of its Azure DevOps System

Overview of Operations

Business Description

Azure DevOps provides a set of cloud-powered collaboration tools that work with customers' existing Integrated Development Environment (IDE) or editor, to enable engineering teams to work effectively on software projects of diverse shapes and sizes.

Azure DevOps supports many customers and partner organizations on collaborative software development projects by providing source control, project-tracking tools for agile teams and continuous integration functionality. Azure DevOps is designed to meet their security, privacy, and compliance requirements.

Azure DevOps is designed to provide *confidentiality, integrity, and availability* of customer data. It also provides transparent *accountability* to allow customers and their agents to track administration of services.

Applicability of Report

This report has been prepared to provide information on internal controls of Microsoft that may be relevant to customers pursuing the security, availability, processing integrity, and confidentiality trust services criteria. Microsoft has considered the service-specific characteristics and commitments to determine applicability of the SOC 2 Trust Services Criteria for the in-scope features. Based on the guidance from AICPA, the following are the applicability considerations:

Trust Services Criteria	Description	Applicability Considerations
Security	Addresses risks related to potential abuse, theft, misuse, and improper access to system components	Applies to features that store, process, or transmit customer data
Availability	Addresses risks related to system accessibility for processing, monitoring and maintenance	Applies to features whose accessibility is advertised or committed by contract or by Service Level Agreement (SLA)
Processing Integrity	Addresses risks related to completeness, accuracy, and timeliness of system / application processing of transactions	Applies to features that process user-initiated or system-initiated events
Confidentiality	Addresses risks related to unauthorized access or disclosure of specific information designated as "confidential" within contractual arrangements	Applies to features that store, process, or transmit customer data

Trust Services Criteria	Description	Applicability Considerations
Privacy	Addresses risks related to protection and management of personal information	Not applicable since financial and personal information of customers is collected and handled within Microsoft Online Services Customer Portal (MOCP), which is outside the scope of the Azure DevOps system boundary

As such, the detail herein is intended to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each customer may consider important. Furthermore, detail is limited to the controls in operation to support the features as defined in the Report Scope and Boundary described below. The authorized users of the system providing these features are limited to Azure DevOps personnel.

Report Scope and Boundary

This report covers the following Azure DevOps features including infrastructure, development, operations, and support for Azure DevOps:

1. Team Foundation Service (TFS)
 - a. Azure Boards
 - b. Azure Repos
 - c. Azure Pipelines
 - i. Release Management (RM)
2. Shared Platform Services (SPS)
 - a. Account & Authorization
 - b. Identity
 - c. Licensing
 - d. Profile
 - e. Token
3. Azure Test Plans
4. Azure Artifacts
 - a. Packages
 - b. Feeds
 - c. Blob Storage
5. Service Hooks (SH)
6. Code Search

Principal Service Commitments and System Requirements

Microsoft makes service commitments to its customers and has established system requirements as part of the Azure DevOps service. Some of these commitments are principal to the performance of the service and relate to applicable trust services criteria. Microsoft 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 Microsoft’s service commitments and system requirements are achieved.

Service commitments to customers are documented and communicated in [Service Level Agreements](#) (SLAs) and other customer agreements such as the [Microsoft Product Terms](#), [Licensing Use Rights](#), [Microsoft Privacy Statement](#), and [Microsoft Trust Center](#), as well as in the description of the service offering provided online. Service commitments include, but are not limited to, the following:

- Security: Microsoft has made commitments related to securing customer data and complying with relevant laws and regulations. These commitments are addressed through measures including data encryption, authentication mechanisms, physical security and other relevant security controls.
- Availability: Microsoft has made commitments related to percentage uptime and connectivity for Azure DevOps as well as commitments related to service credits for instances of downtime.
- Processing Integrity: Microsoft has made commitments related to processing customer actions completely, accurately and timely. These customer actions include, for example, specifying geographic regions for the storage and processing of customer data or executing load tests by specifying customized parameter sets.
- Confidentiality: Microsoft has made commitments related to maintaining the confidentiality of customers’ data through data classification policies, data encryption and other relevant security controls.

Microsoft has established operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Azure DevOps’ 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 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 various Azure DevOps features.

Azure DevOps Environment

Azure DevOps is developed and managed by the Azure DevOps team and is part of the Microsoft Cloud and Artificial Intelligence (C+AI) division. Azure DevOps uses Microsoft Azure (“Azure”) as a cloud platform and datacenter services to host its features. Azure DevOps provides and manages the application and data that reside on the Azure platform. Azure DevOps continues to be part of Microsoft’s Cloud + Artificial Intelligence (C+AI) division and follows similar controls and processes as other services within C+AI. The following diagram shows a high level “stacked view” of the Azure DevOps environment.

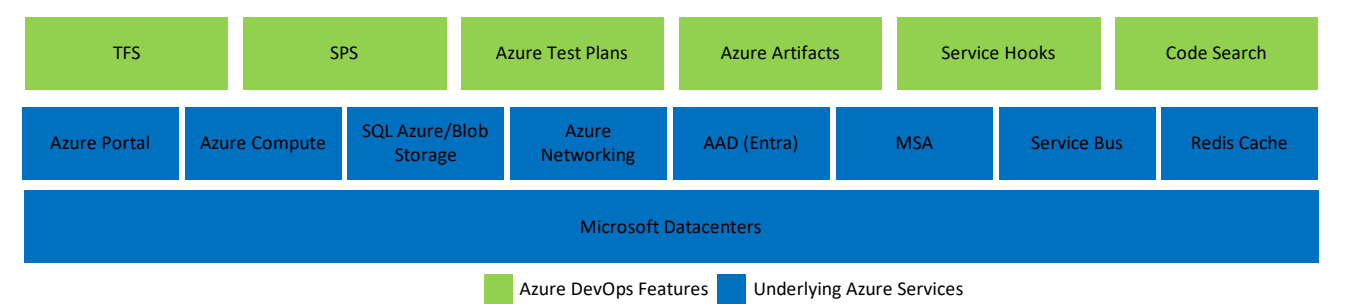


Figure 1: Azure DevOps Architecture - Stacked View

Features and Software Overview

Azure DevOps provides a set of cloud-powered collaboration tools for teams that develop software projects. Azure DevOps provides features for teams to share code, track work, and ship software by complementing the IDE. The following diagram shows an overview of Azure DevOps features and key components.

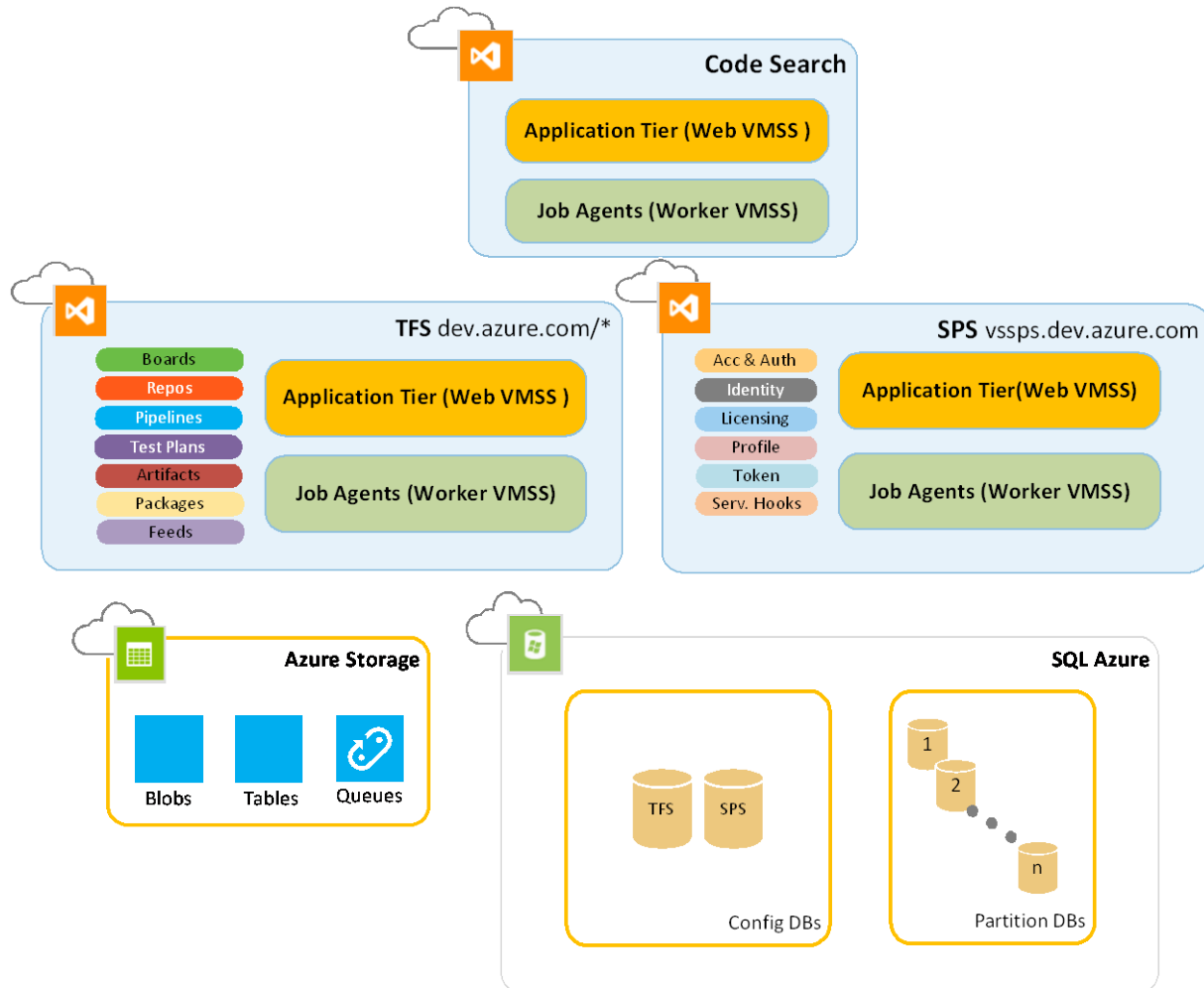


Figure 2: Azure DevOps Core Infrastructure

- **Team Foundation Service (TFS):** TFS is a cloud-powered product offering:
 - **Azure Boards:** Azure Boards provides agile tools to plan, track and discuss work across teams.
 - **Azure Repos:** Azure Repos are cloud-hosted private Git repos and can also be used to collaborate to build better code with pull requests and advanced file management.
 - **Azure Pipelines:** Azure Pipelines can be used to build, test, and deploy with continuous integration and deployment (CI/CD) that works with any language, platform, and cloud. It can also be used to connect to GitHub or any other Git provider and deploy continuously.
 - **Release Management (RM):** Release Management is a DevOps solution to automate deployments as well as workflows, apply security policies, manage users and retain full traceability.
- **Shared Platform Services (SPS):** SPS provides features which are not Azure DevOps-specific, such as account authentication and authorization, licensing services, identity, profile, and token services.

- **Azure Test Plans:** Azure Test Plans is used to test and ship code using manual and exploratory testing tools.
- **Azure Artifacts:** Azure Artifacts is a tool to create, host, and share packages, and add artifacts to CI/CD pipelines.
- **Service Hooks (SH):** Service Hooks uses the Representational State Transfer (REST) Application Programming Interfaces (APIs) to programmatically create subscriptions and notify customer service when a specific event in a team project occurs.
- **Code Search:** Code Search provides fast, flexible and accurate search across all code.

Microsoft Azure

The Azure DevOps production infrastructure is hosted on Azure and located in globally distributed Microsoft datacenters. Azure is responsible for the physical security of the datacenters, data protection, physical hardware asset management, and network services. These datacenters are managed, monitored, and operated by Microsoft operations staff delivering online services 24x7x365. Azure DevOps operates out of the Microsoft datacenters located in the following regions:

- North America
 - East US
 - East US 2
 - West US
 - West US 2
 - West Central US
 - Central US
 - South Central US
 - North Central US
 - Canada Central
- Europe
 - West Europe
 - North Europe
 - UK South
- South America
 - Brazil South
- Asia
 - South India
 - Southeast Asia
- Australia
 - Australia East

Azure also maintains and manages network and platform security. Azure DevOps incorporates security practices at the application layer to enhance security for Azure DevOps customers. Azure and its associated controls implemented to satisfy the in-scope trust services criteria, are not in scope for this report.

Microsoft Online Services Customer Portal and Microsoft Accounts / Organizational Accounts

Users who have access to Azure DevOps have established authentication and authorization privileges based on their Microsoft Accounts (MSA), GitHub Accounts and/or Organizational Accounts. Azure DevOps customer billing is handled by Azure and the Microsoft Online Services Customer Portal (MOCP). MOCP and MSA or Organizational Accounts and GitHub Accounts and their associated authentication mechanisms are not in scope for this report.

Core Service Engineering (CSE)

Core Services Engineering (CSE) is an internal Microsoft business unit that is responsible for activities related to managing and operating Microsoft's worldwide internal technologies infrastructure, corporate and product information, product production and distribution, and maintenance of key internal systems.

Azure is responsible for hosting and managing resource domains for Azure DevOps and is carved-out from the scope of this report.

Azure DevOps Infrastructure

Azure DevOps runs on the Azure Platform as a Service (PaaS) environment. Azure DevOps uploads the Azure DevOps application using Azure's Management APIs. Azure handles the service management from provisioning to load balancing and health monitoring for continuous availability.

Azure DevOps components are implemented as one or more Azure Virtual Machine Scale Sets (VMSS) instances emulating the role of Application Tier (AT) or Job Agent (JA).

- 1. Application Tier (Web VMSS):** ATs are Azure web VMSS that interact with customers directly through Web browsers or other HTTP clients.
- 2. Job Agent (Worker VMSS):** JAs are Azure worker VMSS for more general use, and designed to run a variety of backend jobs.

Once an application is running, Azure continues to monitor it at the infrastructure level. If the code fails, the role instance crashes, or the physical machine which the instance is executing on fails, Azure automatically starts a new instance of this role.

Data & Storage

Azure DevOps uses Azure SQL Database for relational storage. Azure DevOps controls its data and access to the data. The Azure SQL Database team handles the administrative work, such as managing the hardware infrastructure and automatically keeping the database and operating system software up to date. Databases are automatically replicated with 1 master and 3 secondary replicas to address failures. A secondary instance of the database is promoted to primary in case the initially designated primary instance fails.

Azure DevOps also uses Azure Storage Service blobs, tables and queues. Azure Storage accounts have redundant data copies in a pair region for fault tolerance.

Azure DevOps Supporting Infrastructure

Deployment Boxes

Deployment boxes are primarily used by Release Management (RM) feature to deploy Azure DevOps, as well as customer applications in the Azure cloud. These VMSS servers also function as utility servers for manual deployments, debugging, deploying new Azure DevOps instances, managing certificates, and collecting diagnostics information from production systems.

Deployment boxes are infrastructure components used internally by the Azure DevOps Observability team to access the production environment. There is no storage of customer data within the deployment boxes.

People

Azure DevOps is comprised and supported by the following personnel who support in the delivery and management of its cloud-based services:

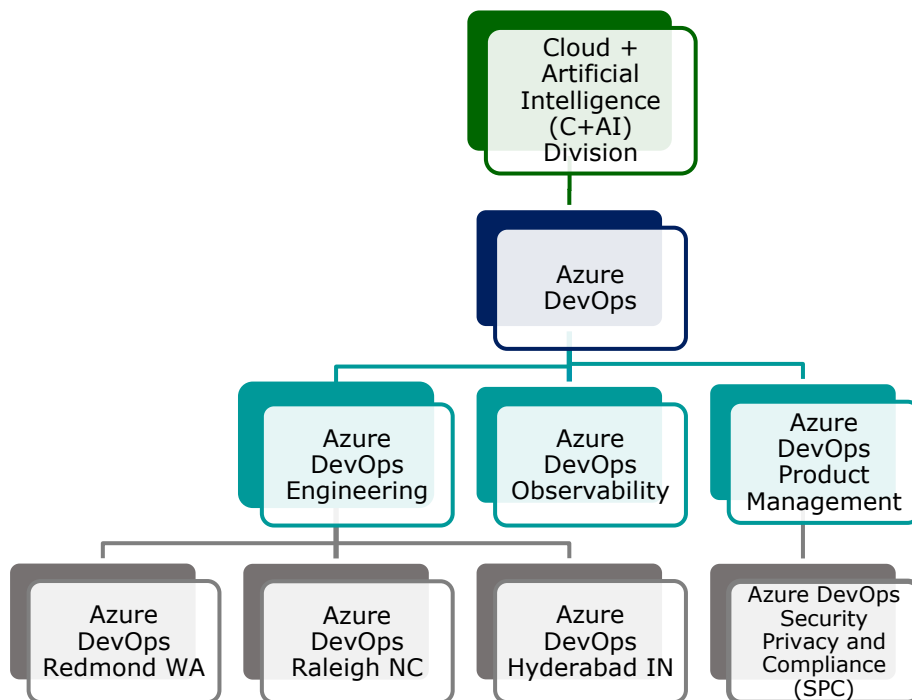


Figure 3: Azure DevOps Organization Structure

Azure DevOps Engineering Team

The Azure DevOps engineering teams include personnel from the development, test, and Product Management (PM) disciplines for designing, developing, and testing of features and for providing technical support as needed.

The Engineering teams manage the component life-cycle as well as monitor and support their specific services and features. Their responsibilities include:

- Deploying new features
- Providing operational support for existing features (DevOps model)

- Proactively addressing potential platform and service issues
- Reacting to incidents and support requests

Azure DevOps Observability Team

The Azure DevOps Observability team is responsible for the infrastructure that provides operational and business data/insights to Azure DevOps and its stakeholders. Their responsibilities include:

- Enabling the ability to monitor service health and investigate root cause for live site incidents
- Supporting the cadence of business reporting and enabling data driven analysis
- Providing guidance and enabling self-service so teams can enable telemetry and gain insights from exploring the resulting data

Azure DevOps Product Management Team

The Azure DevOps Product Management (PM) team is focused on feature development for the various Azure DevOps features. The Security, Privacy and Compliance (SPC) team sits within the PM team and is responsible for developing, maintaining and monitoring the Information Security (IS) Program including the Risk Assessment process. As part of managing compliance adherence, the team drives compliance and security related features within Azure DevOps.

The SPC team works to make Azure DevOps a secure and compliant cloud platform by building common security technologies, tools, processes and best practices across Azure DevOps. The SPC team is also involved in the review of enhancements of Azure DevOps features to facilitate security considerations during the Secure Development Lifecycle (SDL). This team is also responsible for:

- Assisting with Secure Development Lifecycle
- Assisting with Incident Response
- Driving security functionality and feature development work

Control Environment

Integrity and Ethical Values

Corporate governance at Microsoft starts with an independent Board of Directors that establishes, maintains, and monitors standards and policies for ethics, business practices, and compliance that span the company. Corporate governance at Microsoft serves several purposes:

1. To establish and preserve management accountability to Microsoft's owners by appropriately distributing rights and responsibilities among Microsoft Board members, managers, and shareholders.
2. To provide a structure through which management and the Board set and attain objectives and monitor performance.
3. To strengthen and safeguard a culture of business integrity and responsible business practices.
4. To encourage the efficient use of resources and to require accountability for stewardship of these resources.

Further information about Microsoft's general corporate governance is available on the Microsoft public website.

Microsoft Standards of Business Conduct

The Microsoft Standards of Business Conduct (SBC) reflect a commitment to ethical business practices and regulatory compliance. They summarize the principles and policies that guide Microsoft's business activities and provide information about Microsoft's Business Conduct and Compliance Program. The SBC was developed in full consideration of Sarbanes-Oxley and proposed NASDAQ listing requirements related to codes of conduct. Additional information about Microsoft's SBC is available on the Microsoft public website.

Training

Annual SBC training is mandatory for all Microsoft employees and contingent staff. The SBC training includes information about Microsoft corporate policies for conducting business while conforming to applicable laws and regulations. It reinforces the need for employees to work with integrity and to comply with the laws of the countries where Microsoft operates. It also guides employees and contingent staff on how to report possible violations and find contact information if they need to report a violation or ask questions. Microsoft also trains its outsourced providers to understand and comply with Microsoft's supplier code of conduct.

Microsoft employees are also encouraged to attend in person or virtual security training on an annual basis. The objective of these trainings is to educate engineers on secure design and operations that align with Microsoft's security principles and strategy. These training sessions also aim to increase awareness of security threats.

Microsoft recognizes that cyber-attacks and data breaches are real security threats that all enterprises face. Microsoft believes that every Microsoft employee plays a role in enhancing customer trust and protecting the Microsoft brand by following sound security practices. These courses are designed to help employees detect and prevent threats to the corporate network.

Accountability

All Microsoft and contingent staff are accountable for understanding and adhering to the guidance contained in the Microsoft Security Policy and any applicable supporting procedures. Individuals not employed by Microsoft, but allowed to access, manage, or process information assets of the Azure DevOps environment are also accountable for understanding and adhering to the guidance contained in the Security Policy and procedures.

Commitment to Competence

Microsoft hiring managers define job requirements prior to recruiting, interviewing, and hiring. Job requirements include the primary responsibilities and tasks involved in the job, background skills needed to perform the job, and personal qualifications desired. Once the requirements are determined, managers create a job description, which is a profile of the job and is used to identify potential candidates. When viable candidates are identified, the interview process begins to evaluate candidates and make an appropriate hiring decision.

Microsoft employees create individual core priorities that align with those of their manager, organization, and Microsoft, and are supported with customer-centric actions and measures so that everyone is working toward the same overarching vision. Core priorities are established when employees are hired, and then updated throughout the year during one-on-one connect meetings with their manager. The primary focus of the connect meetings is to assess employees' performance against their core priorities and to agree on an updated list of priorities going forward. A manager uses this evaluation of an individual employee's impact, taking into consideration what was accomplished, how the results were achieved and the demonstration of priorities relevant to the role.

Microsoft's Compensation Committee is responsible for reviewing and discussing plans for executive officer development and corporate succession plans for the CEO and other executive officers.

Compliance and Ethics – Board of Directors and Senior Leadership

The Compliance and Ethics designs and provides reports to the Board of Directors on compliance matters. Compliance and Ethics also organizes annual meetings with the Senior Leadership Team (SLT) for their compliance review.

Internal Audit Department

Microsoft has an Internal Audit (IA) function which consists solely of independent directors who report directly to the Audit Committee (AC) of the Board of Directors. IA has a formal charter that is reviewed by the AC and management. Responsibilities of IA include performing audits, reporting issues, and making recommendations to management and the AC.

Audit Committee

The AC Charter and Responsibilities are published on Microsoft's website. The AC meets privately on a quarterly basis with Microsoft's external auditors and IA. The agendas for the quarterly AC meetings are found in the AC Responsibilities Calendar sent out with the Charter. In addition, the AC influences the company through the IA function. The AC reviews the scope of internal audit and assists in the process of identifying and resolving any issues. Lastly, the AC monitors itself by completing an annual self-evaluation.

Risk Assessment

Practices for Identification of Risk

The Microsoft Enterprise Risk Management (ERM) function provides management and accountability of Microsoft Corporate's short- and long-term risks. ERM collaborates with Internal Audit, Financial Compliance Group, Operations, and Legal and Compliance groups to perform a formal risk management process. Risk assessments include risks in financial reporting, fraud, and compliance with laws.

Further, Azure DevOps performs a risk assessment of each feature on a rotating semi-annual basis, including potential hazards such as access monitoring, broad data breach, malware attacks, and privacy. Additionally, Azure DevOps performs a holistic risk assessment of the platform on an annual basis. Threats are evaluated for impact on the security, continuity, and operations of the Azure DevOps platform.

Internal Audit - Fraud Risks

IA and the Financial Integrity Unit (FIU) are responsible for identifying fraud risks across Microsoft. The FIU performs procedures for the detection, investigation, and prevention of financial fraud impacting Microsoft worldwide. Fraud and abuse that is uncovered, is reported to the Disclosure Committee. The FIU provides both a reactive and proactive response to allegations of fraud and abuse. The FIU uses a case management system that is also used by the Director of Compliance to track cases and related metrics. The FIU interacts with Microsoft management, Corporate, External, and Legal Affairs (CELA), Human Resources (HR), Finance, Procurement, and others to determine specific fraud risks and responses.

Periodic Risk Assessment

The Microsoft Internal Audit team and other groups within the company perform a periodic risk assessment. The assessment is reviewed by senior management.

IA specialization area leaders determine high-priority risks across the company, including financial reporting, operational business process, and systems controls. Control failures are also assessed to determine whether they give rise to additional risks.

Compliance and Ethics/ Internal Audit / Risk Management - Risk Responsibility

The responsibility for risk is distributed throughout the organization based on the individual group's services. Compliance and Ethics, IA, and the ERM teams work together to represent enterprise risk management. Through quarterly and year-end reviews, the Chief Financial Officer (CFO) and Corporate Controller (and respective groups) review the disclosures and issues that may have arisen.

Monitoring

Azure DevOps Security and Compliance Monitoring

Azure DevOps maintains reasonable and appropriate technical and organizational measures, internal controls, and information security routines intended to help protect customer data against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction.

Subservice Organization Monitoring

Azure DevOps utilizes the internal subservice, Azure, which provides cloud services and datacenter hosting services. Azure DevOps' management assesses the risks associated with the subservice organization and has implemented various management oversight and monitoring processes to ascertain that the organization continues to provide services in a controlled manner. These include, but are not limited to, reviewing third-party service auditor reports and holding discussions with subservice organization's management.

Compliance and Ethics - Business Conduct Hotline

There is a confidential and anonymous Business Conduct Hotline available for employees to report issues. The hotline is accessible 24x7 through email, phone, fax, and mail. The individual may also send a letter or fax reporting the concern to Microsoft's Director of Compliance.

Employees are instructed that it is their duty to promptly report any concerns of suspected or known violations of the *Code of Professional Conduct*, the SBC, or other Microsoft policies or guidelines. The procedures to be followed for such a report are outlined in the SBC, and the Whistle Blowing Reporting Procedure and Guidelines in the Employee Handbook. Employees are also encouraged to communicate the issue to their manager, their manager's manager, their CELA contact, their HR contact, or the Compliance Office.

Internal Audit

Microsoft's IA department provides support to management across the company by independently and objectively assessing whether the objectives of management are adequately performed, and by facilitating process improvements and the adoption of business practices, policies, and controls governing worldwide operations.

Information and Communication

An annual process exists to set objectives and commitments among all executives and is rolled down to employees. These commitments and objectives are filtered down to team members through the annual and mid-year review processes.

Internal Communication

Responsibilities around internal controls are communicated broadly through Monthly Controller calls, All Hands Meetings run by the Chief Financial Officer (CFO), and email updates sent / conference calls held by the Financial Compliance Group with the Sarbanes-Oxley extended project team. Responsibilities for compliance with policies are outlined in the SBC training.

Office of the CFO - Communications External to the Company

CFO communications outside the company occur throughout the year and, where appropriate, these external communications include a discussion of the company's attitude towards sound internal controls. The Office of the CFO is responsible for communications outside the company such as Quarterly Earnings Release, Financial Analyst meetings, customer visits, external conferences, and external publications.

Data

Customers upload data to store or process in Azure DevOps. In addition, certain types of data are provided by the customers or generated on the customer's behalf to enable the use of the Azure DevOps components. Microsoft only uses customer data to support the provisioning of the services subscribed to by the customers in accordance with the Service Level Agreements. The customer-provided data is broadly classified into the following data types:

- 1. Access Control Data** is data used to manage access to other types of data or functions within Azure DevOps.
- 2. Customer Content** is the data, information, and code that Microsoft internal employees, and non-Microsoft personnel (if present) provide to, transfer in, store in or process.
- 3. End-user Identifiable Information (EUII)** is data that directly identifies or could be used to identify the authenticated user of a Microsoft service. EUII does not extend to other personal information found in Customer Content.
- 4. Support Data** is data provided to Microsoft and generated by Microsoft as part of support activities.
- 5. Feedback** is data provided as part of a review or feedback for one of Microsoft's products and services that includes personal data.
- 6. Account Data** is information about payment instruments. This type of data is not stored in the Azure DevOps platform.
- 7. Public Personal Data** is publicly available personal information that Microsoft obtains from external sources.
- 8. End User Pseudonymous Identifiers (EUPI)** are identifiers created by Microsoft tied to the user of a Microsoft service.
- 9. Organization Identifiable Information (OII)** is data that can be used to identify a particular tenant / Azure DevOps organization.
- 10. System Metadata** is data generated in the course of running the service, not linkable to a user or tenant. It does not contain Access Control Data, Customer Content, EUII, Support Data, Account Data, Public Personal Data, EUPI, or OII.

11. Public Non-Personal Data is publicly available information that Microsoft obtains from external sources. It does not contain Public Personal Data.

The following table illustrates some examples of the different data elements provided by the customer with respect to the in-scope Azure DevOps features.

Azure DevOps Feature	Data Element	Data Type
TFS	Azure Boards: Work Items	Customer Content
	Azure Boards: Work Item Attachments	Customer Content
	Azure Repos: Source Code	Customer Content
	Azure Pipelines: Release Definitions	Customer Content
	Microsoft Server Names / Server IPs	System Metadata
SPS	Account & Authorization: Storage Keys & Account Passwords	Access Control Data
	Profile: Customer Profile Data	Customer Content
	Profile: Internet Protocol Address and Email Address	End-user Identifiable Information (EUII)
	Token: Authentication Token Hashes	Access Control Data
Azure Test Plans	Test Data and Results	Customer Content
Azure Artifacts	Package Data and Feeds	Customer Content
Service Hooks	Storage Keys & Account Passwords	Access Control Data
Code Search	Storage Keys & Account Passwords	Access Control Data
	Source Code Indices	Customer Content

Data Ownership

Customer data is handled and stored in accordance with the accepted standards for the service. Microsoft does not claim ownership over customer data or information that passes through the Azure DevOps service or that is hosted in its repositories. The Azure DevOps Terms and Conditions ([Microsoft Product Terms](#)) cover the agreement with the customers regarding data ownership. Further, customer data is accessible within agreed upon services in data formats compatible with providing those services.

Applicable Data Elements

For the purposes of this report, Microsoft has implemented controls to protect the data elements specifically covered under Customer Content and Access Control Data.

Description of Controls

Security Organization - Information Security Program

Azure DevOps has established an Information Security Program that provides documented management direction and support for implementing information security within the Azure DevOps environment. The design and implementation of applicable controls are defined based on the type of Azure DevOps feature and its architecture.

The objective of the Information Security Program of Azure DevOps is to maintain Confidentiality, Integrity, and Availability (CIA) of information while complying with applicable legislative, regulatory, and contractual requirements.

The Information Security Program consists of the following components:

1. Policy, Standards and Procedures
2. Risk Assessment
3. Training and Awareness
4. Security Implementation
5. Review and Compliance
6. Management Reporting

The Information Security Program is based on the International Organization of Standards (ISO) Codes of Practice for information security management ISO/IEC 27001:2013 standard. Its accompanying policies and processes provide a framework to assess risks to the Azure DevOps environment, develop mitigating strategies and implement security controls. In addition, team-specific Standard Operating Procedures (SOPs) are developed to carry out specific operational tasks in the following areas:

1. Access Control
2. Asset Management
3. Business Continuity and Disaster Recovery
4. Capacity Management
5. Cryptographic Controls
6. Document and Records Management
7. Exception Process
8. Change and Release Management
9. Incident Management
10. Legal and Regulatory Compliance
11. Logging and Monitoring
12. Secure Development Lifecycle
13. Third Party Management
14. Vulnerability Scanning and Patch Management

Information Security Policy

Azure DevOps adheres to Microsoft's Information Security Policy (MSP) that addresses security, availability and confidentiality for Azure DevOps. The Information Security Policy outlines high level objectives related to information security, defines risk management requirements and information security roles and responsibilities. The policy contains rules and requirements that must be adhered to in the delivery and support of Azure DevOps components. SOPs are developed to support the policy. The policy is communicated to employees, contractors and third-parties.

The Azure DevOps Information Security Management Forum (ISMF), which is comprised of stakeholders and representatives from Security, Engineering, Operations as well as supporting business functions (e.g., CELA, and HR), reviews and provides input into the Microsoft Information Security Policy.

The policy is reviewed and updated, as necessary, at least annually, or more frequently, in the event of a significant security event, or upon significant changes to the service or business model, legal requirements, organization or platform.

Each management-endorsed version of the MSP and subsequent updates are distributed to relevant stakeholders from Azure DevOps Security and Compliance intranet site.

Information System Review

Azure DevOps performs a periodic Information Security Management System (ISMS) review and results are reviewed with the management. ISMS documents cover scope, declaration of applicability and the results of the last management review. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.

Compliance Requirements

Azure DevOps maintains reasonable and appropriate technical and organizational measures, internal controls, and information security routines intended to help protect customer data against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction. Azure DevOps compliance requirements are monitored and reviewed regularly with CELA and other internal organizations, as applicable. Members of the Azure DevOps SPC, Azure Compliance, and Cloud + AI Security teams update relevant SOPs, Security Policy and service descriptions in order to remain in-line with compliance requirements. The Security Policy requires a periodic review of the performance of policies and procedures governing information security. The Compliance team coordinates independent third-party audits (internal and external) which evaluate systems and control owners for compliance with security policies, standards, and other requirements. Audit activities are planned and agreed upon in advance by stakeholders, including approval for necessary read access required to perform such audits to avoid impacting the overall availability of the service. External independent audits are performed at least annually and any findings are prioritized and tracked to resolution.

Personnel

Microsoft performs employee background screening as determined by the hiring manager based on access to sensitive data, including access to personally identifiable information or to back-end computing assets and according to customer requirements, as applicable. For contractors or contingent staff, vendor companies are required to conduct background screening. Microsoft also employs a formal performance review process to ensure employees adequately meet the responsibilities of their position, including adherence to company policies, information security policies, and workplace rules. Hiring managers may, at their discretion, initiate corrective actions, up to and including immediate termination, if any aspect of an employee's performance and conduct is not satisfactory.

Corporate policies are communicated to employees and relevant external parties during the onboarding process and as part of an annual security training and awareness education program. Non-disclosure agreements are signed by employees and relevant external parties upon engagement with Microsoft. Disciplinary actions are defined for persons who violate the security policy or commit a security breach. Security policy and non-disclosure requirements are reviewed periodically to validate appropriate protection of information.

Training and Awareness

Information security training and awareness is provided to Azure DevOps employees, contractors and third-parties on an ongoing basis to educate them on applicable policies, standards and information security practices. Awareness training on security, availability and confidentiality of information is provided to Azure DevOps employees at the time of joining as part of induction. In addition, Azure DevOps staff participate in a mandatory security, compliance, and privacy training periodically in order to design, build, and operate secure cloud services. Please refer to the previous section on training for details.

Employees receive information security training and awareness through different programs such as new employee orientation, computer-based training, and periodic Azure DevOps communication (e.g., compliance and security program updates). These include training and awareness pertaining to Azure DevOps, in the security, availability, confidentiality, and integrity domains. In addition, job-specific training is provided to Azure DevOps personnel, where appropriate. The key objectives of the information security training and awareness program are listed below:

- The learner will be able to articulate the need to protect confidentiality, integrity, and availability of the Azure DevOps environment.
- The learner will be able to apply basic security practices to safeguard the Azure DevOps environment and customer information.
- The learner will understand the criticality of security, compliance and privacy in relation to customer expectations.
- The learner will have a basic understanding of Azure DevOps' responsibility to meet compliance and privacy commitments.
- The learner will know where to find additional information on security, privacy, and compliance.

Roles and Responsibilities

Information security roles and responsibilities are defined across the different Azure DevOps functions. The cross-functional Azure DevOps ISMF is responsible for information security matters and they discuss, review and coordinate security activities across Azure DevOps. In addition, the Azure DevOps Security team facilitates implementation of security controls and provides security guidance to the Azure DevOps teams. The Azure DevOps Security, Privacy and Compliance team coordinates with representatives from CELA (legal, compliance requirements, secure development and privacy), HR (personnel security) and Azure (security policy requirements) on additional information security related activities impacting the Azure DevOps service.

Risk Management

Azure DevOps has developed and documented a risk assessment policy to address the purpose, scope, roles, and responsibilities for managing deviations from the security policies/standards. The risk assessment policy and procedures are reviewed and updated on an annual basis. Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within the Azure DevOps environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., CELA, Procurement) in reviewing risks associated with external parties and establishing relevant agreements. Prior to contracting with Microsoft, suppliers undergo a risk assessment based

on the services that will be provided and data handled. The list of reviewed suppliers is maintained, and their risk profiles are reviewed at least annually.

Azure DevOps Compliance

Microsoft Azure DevOps supports compliance with a broad set of industry-specific laws and meets broad international standards. Azure DevOps has ISO 27001 and ISO 27018 certifications. Operated and maintained globally, Microsoft Azure DevOps is regularly and independently verified for compliance with industry and international standards and provides customers the foundation to achieve compliance for their applications. More information is available from the Microsoft Trust Center.

Communications

Policies Communication

Azure DevOps maintains communication with employees using the corporate intranet sites, emails, and trainings etc. The communications include, but are not limited to, communication of Azure DevOps policies and procedures, corporate events, new initiatives, and awareness on ISMS and Business Continuity Management System. Changes and updates to Azure DevOps policies and procedures, and all subsequent updates are distributed to all relevant stakeholders from the Azure DevOps SPC intranet site.

Service Level Agreements

Azure DevOps details commitments made regarding delivery or performance of services. Details are published in the Service Level Agreements (SLAs) available for the service on the following website: [Service Level Agreements](#)

Customer Communication

Prior to engaging Azure DevOps services, customers are required to review and agree with the acceptable use of data and the Azure DevOps service, as well as security and privacy requirements, which are defined in the Microsoft Online Services Use Rights, Microsoft Online Subscription Agreement, Azure DevOps Privacy Statement, and Azure DevOps Terms and Conditions.

Subsequent communication with customers is primarily achieved through the website [Azure DevOps](#).

- [Service Health Dashboard](#) - Azure DevOps maintains and notifies customers of potential changes and events that may impact security, availability, or confidentiality of the service through an online Service Health Dashboard. The Service Health Dashboard is used to disclose the nature, timing, extent, and disposition of the incidents impacting various Azure DevOps services. The online Service Dashboard is updated in real-time and RSS feeds are also available for subscription. The Status History section allows customers to inquire about past events as well as postmortem details.
- [Legal](#) - Any changes / updates to the Service Agreement, Terms, End User License Agreement (EULA), Acceptable Use Policy (AUP), Privacy Statement or SLAs are posted on the Azure website. The information presented in the Microsoft Trust Center is current as of the "Last Updated" date at the top of each section, but is subject to change without notice. Customers are encouraged to review the Microsoft Trust Center periodically to be informed of new security, privacy and compliance developments.
- [Contact Information](#) - Customers are able to communicate with Azure DevOps support in various ways. The contact section presents forum access and direct contact for support.

Details around confidentiality and related security obligations for customer data and guidelines and recommendations for the secure use of the cloud services is communicated through the Azure DevOps Data Protection whitepaper (<https://aka.ms/AzureDevOpsSecurity>) and Microsoft Trust Center (<https://www.microsoft.com/en-us/trust-center/product-overview>).

Azure DevOps maintains a customer support website containing detail for customers and other third-parties to inform about potential security issues and submit complaints. Reported issues are reviewed and addressed according to documented incident management procedures. Incidents for Azure DevOps are triaged by the appropriate team members for review and resolution.

Procedures to evaluate government investigative demands for customer data are established and documented. Procedures include a review and assessment by the Microsoft legal department, which will evaluate the legal basis for the request to determine what response is required, and notify the impacted customer where permitted by law. Where Microsoft is required to produce customer data, the minimum data responsive to the request as required by law is produced. These procedures are reviewed at least on an annual basis.

Incident Management

Azure DevOps has implemented an incident management framework that includes defined processes, roles, communications, responsibilities and procedures for detection, escalation and response to incidents internally and to customers.

Incident Internal Monitoring and Communication

The Azure DevOps Observability and Engineering teams' processes are crafted to ensure focus on service health and customer experience that minimizes the time to detect, respond to and mitigate impacting issues. Ownership for Live Site is shared across all Engineering disciplines. This results in process improvements, which evolve out of the direct experience, in the areas of monitoring, diagnostics, resiliency, and quality assurance.

Live Site management in Azure DevOps is broken into three distinct tracks. The first track describes that the events are monitored and alerted. The second track lays out the process for handling incidents. The third track focuses on pulling out the learnings from each incident and to drive continual improvements into service Live Site health. Azure DevOps has a weekly cadence for review of Live Site Incidents (LSI).

Telemetry	Incident Management	Live Site Review
<ul style="list-style-type: none"> • Alerts - Define health alerts for failure modes • Diagnostics - Deliver instrumentation data and operational reports • Troubleshooting Guides - Guidance for investigation an alert is defined by the feature and then refined by the Engineering team • Failure Mode Testing - The Observability team performs failure testing to ensure alerts fire as expected • Onboarding - The Feature team works with their Service Engineers to onboard new alerts to be sent to the 24 x7 team 	<ul style="list-style-type: none"> • Detection - Product alerts start the Live Site Incident (LSI) process upon detection of health issues • Triage - The 24x7 team receives all critical alerts and confirms impact using TFS guidance • Escalation - Both Dev and Ops have individuals in the on-call rotation. Engineering team is the initial escalation path. Engineering team calls Dev as needed • Incident Management - A bridge is managed by the Engineering team which engages Dev and Partners to troubleshoot • Resolution - Communication and service restoration are actively driven until customer 	<ul style="list-style-type: none"> • Goal - Monthly review of LSI ensures that Leadership has visibility into live site health and repeat issues • Cadence - Incidents have root cause documented and are reviewed on a weekly basis • Audience - Azure DevOps Leadership and Partners attend to drive impact; Developers attend to provide details on service incidents • Ownership - Dev owns reviews for App and Deploy issues; Observability team owns reviews for Platform issues • Driving Improvements - Bugs and problem work items are logged for gaps (e.g., missing alerts) and repeat root cause

Figure 4: Incident Management

Incident Handling

The Azure DevOps team uses the established incident classification, escalation and notification process for assessing an incident's criticality and severity, and accordingly escalating to the appropriate groups for timely action. The Azure DevOps Live Site team, with assistance from additional Azure DevOps and Microsoft teams (e.g., Cloud + AI Security team for investigation, when necessary), documents, tracks, and coordinates response to incidents. Where required, security incidents are escalated to the privacy, legal or executive management team(s) following established forensic procedures to support potential legal action after an information security incident.

Incident Post-mortem

Post-mortem activities are conducted for customer impacting incidents with high severity ratings (i.e., severities 0, 1, and 2) and security incidents. The post-mortems are reviewed by the Azure DevOps Engineering team during monthly review meetings with Azure DevOps senior management. Incident and security post-mortem trends are reviewed and evaluated on a periodic basis and, where necessary, the Azure DevOps service or security program may be updated to incorporate improvements identified because of incidents.

Logical Access

Customer Registration

Azure DevOps customers register with Azure DevOps by setting up an account through the Azure DevOps portal using their Microsoft Account (MSA), an Organizational Account (AAD) or GitHub credentials. Azure DevOps logically segregates these customer accounts to restrict unauthorized access. Microsoft Online Services

Customer Portal (MOCP), including billing and registration, and MSA, including password management, are outside the scope of this system description.

Customer Authentication

Azure DevOps customers can login to Azure DevOps with a MSA, an Organizational Account or GitHub credentials. Once the customer is authenticated to Azure DevOps, the customer is given a OpenID cookie that is valid only for a stipulated period. The service forces the customer to obtain a new cookie on a periodic basis. OpenID tokens are used by the browser and the client to communicate with Azure DevOps. Azure DevOps' extensibility model exposes APIs based on REST, SOAP, OAuth, JSON and Service Hooks. Azure DevOps APIs can be accessed directly outside the browser. Azure DevOps has published a standard set of APIs with an ecosystem of tools and libraries on the Azure DevOps public documentation. Azure DevOps customers can connect to the Azure DevOps APIs using the following ways:

- **OAuth 2.0 Session Tokens:** Customer web applications can also authenticate to REST APIs without having the applications request for their usernames and passwords repeatedly. Azure DevOps uses the OAuth 2.0 protocol to authorize customer applications for users and generate access tokens. Customer applications use these tokens to authenticate while accessing REST APIs.
- **Personal Access Tokens:** Applications that require Basic Authentication and non-interactive experiences can use Personal Access Tokens (PATs) to communicate with Azure DevOps. A PAT is an extension to OAuth capabilities. An authenticated user can create a PAT that then enables the user to use Basic Authentication without directly accessing customer credentials. In addition to capabilities of OAuth session tokens, PATs can also be scoped to specific Azure DevOps accounts, and can be revoked when required.
- **SSH authentication:** Customers can connect to Git repos through SSH when the recommended Git Credential Managers or Personal Access Tokens cannot be used to securely connect using HTTPS authentication. SSH public key authentication works with a pair of generated encryption keys.

Additionally, customers can configure settings to allow or deny access through these authentication mechanisms. Customer confidential data such as PATs, Session Tokens and SSH Public Key are hashed and stored securely. Furthermore, user sessions within the service portal expire after a stipulated period of inactivity.

Operator Access

Production Infrastructure Access Management

The Microsoft Security Policy establishes the access control requirements for requesting and provisioning user access for accounts and services. The policy requires that access be denied by default, follow least privilege principle, and be granted only upon business need.

Azure DevOps uses corporate and Azure-managed Active Directory (AD) infrastructure, wherever applicable, for centralized authentication and authorization to restrict access to the systems and features within the Azure DevOps environment.

Domain-account management requests are routed to the designated asset owner or associated agent according to established account provisioning and de-provisioning processes for approval. Typically, access is controlled through domain security groups within the Active Directory in addition to the user's individual accounts. User access requests require approval by the assigned security group owner. Requests for new access are automatically forwarded to the security group owner for approval in the system.

Employee status data from Microsoft HR is used to facilitate the provisioning and removal of user accounts in the corporate and Azure-managed Active Directory domains. Automated feeds from Microsoft HR systems provide this information, and account management processes prevent the creation of an account for individuals

that do not have valid HR records. These feeds also initiate the removal of user accounts for terminated users from the Active Directory. Furthermore, production domain-level user accounts are disabled after a stipulated period of inactivity.

Automated mechanisms are implemented to manage the appropriateness of user access to information systems. Policies and standards for password complexity are established and implemented for Azure DevOps personnel credentials.

Production assets that are not domain-joined or which use local user accounts for authentication, require appropriate approvals prior to being granted access. Manual, periodic reviews of individual accounts, service accounts and security group memberships on assets are performed to evaluate appropriateness of access to information systems, and remediation actions are taken, as necessary, based on the review.

By default, on Azure DevOps Virtual Machines (VMs), user accounts are not created, and the Windows default administrator account is disabled. Temporary access for Azure DevOps personnel to customer data and applications is provisioned based on established procedures with the appropriate approvals. These temporary access events (i.e., request, approval, and revocation of access) are logged and tracked using an internal ticketing system per documented procedures.

Access to Azure DevOps Infrastructure

Azure DevOps maintains a strict control over who has access to the Azure DevOps production environment and customer data. Persistent privileged access to production systems is limited to Observability team members. Production access to the Engineering team members is provided on a temporary basis to resolve Live Site issues. Access is only granted at the level of least privilege, required with a pre-defined expiry, and revoked as soon as the access period expires. Access requests and approvals are tracked and monitored in a separate system.

Access points such as Secure Admin Workstation (SAW) require users to perform two-factor authentication using a smart card and AD domain credentials to gain access. SAW are secure hardened device which limits access to specific users and whitelisted applications. Mobile devices connected to the production environment are limited to Secure Access Workstation (SAW) laptops and do not include phones or tablet.

In the unlikely event where JIT temporary access cannot be used, Azure DevOps service teams have the ability to access the production environment using designated break-glass accounts which provide user a short-term admin level access. Alerting and monitoring has been enabled for all break-glass accounts access. Upon accessing a break-glass account an alert is generated, whereupon the service team will investigate and determine if the access was appropriate.

Remote Desktop

Production servers are configured to require users to perform two-factor authentication using a smart card and domain password to gain access to the Directory Services production servers using the Remote Desktop Connection application. Remote Desktop Connection has encryption settings enforced.

Vulnerability Management

Logging and Monitoring

Azure DevOps uses Azure's agent-based monitoring infrastructure within the Azure platform to provide automated logging and alerting capabilities. The monitoring system detects potential unauthorized activity and security events such as the creation of unauthorized local users, local groups, drivers, services, or IP configurations. The monitoring agents are responsible for monitoring a defined set of user and administrator

events, aggregating log events and sending the aggregated log information to a centralized log repository either at regular intervals or in real-time.

Administrator, operator, and system activities performed within the Azure DevOps environment are logged and monitored. As such, Azure DevOps components are configured to use Coordinated Universal Time (UTC) time and the clocks are synchronized with the domain controller server.

Azure DevOps uses Azure's alerting system to provide real-time alerting through automatic generation of emails and alarms based on the log information captured by the monitoring infrastructure. Feature teams are responsible for configuring the events to be alerted. The event and warning logs are aggregated, alerts are generated on anomalous behavior, and appropriate actions are taken in accordance with the incident handling procedures described in the Incident Management section. Engineering teams manage responses to malicious events, including escalating to and engaging specialized support groups. Also, availability of logging and monitoring software is monitored by internal tools on a continuous basis, and responsible personnel is notified in case of any failure. Logging servers are required to authenticate over encrypted channel to access logs generated within the production environment. Access to logging and monitoring infrastructure is restricted to authorized personnel.

Azure DevOps provides logging mechanisms that can be configured by customers to log activities and metrics.

System Monitoring Tools

1. **Geneva Monitoring** within the Microsoft Azure platform provides automated logging and alerting capabilities for monitoring system use and detection of potential unauthorized activity. Its primary capabilities include Data Collection, Data Aggregation, Data Analysis and Information Access.
2. **Azure Security Monitoring (ASM)** provides logging and alerting upon detection of breaches or attempts to breach Azure cloud-based platform trust boundaries. Critical security event logs generated are configured to alert through Azure's alerting system. ASM monitors key security parameters to identify potentially malicious activity on Azure nodes.
3. **Microsoft Endpoint Protection (MEP)** provides guards against malware that provides security value to the Azure VMSS. Microsoft's antimalware endpoint solutions are designed to run quietly in the background without requiring human intervention. If malware is detected, the endpoint protection agent automatically acts to remove the detected threat.
4. **Windows Defender** guards against malware and helps improve security of the Azure DevOps underlying infrastructure running VMSS running Windows Server 2016 and newer. Windows Defender can be configured to enable antimalware protection for the Azure DevOps virtual infrastructure. Microsoft's antimalware solutions are designed to run quietly in the background without requiring human intervention. If malware is detected, the Windows Defender automatically takes action to remove the detected threat.

In addition, the Azure DevOps Live Site team uses third-party external monitoring services to monitor service health and performance.

Patch Management

Patching of Azure VMSS

Azure DevOps leverages Azure Shared Image Gallery to create custom VMSS images. New images are created on every patch Tuesday, which are used for the creation of new VMSS. Automatic OS upgrade is also enabled to ensure that the latest security fixes and patches are pushed to existing VMSS.

Vulnerability Scanning

C+AI carries out frequent internal scans of Azure DevOps' servers to identify vulnerabilities and assess the effectiveness of the patch management process. The scanning reports are reviewed by appropriate personnel and remediation efforts are conducted in a timely manner.

Baseline Security Configuration for Services

Azure DevOps leverages Azure's established baselines for Azure VMSS. Baselines are actively monitored. Any deviation triggers appropriate notifications, and subsequent remediation activities are performed.

Penetration Testing

Penetration Testing (PEN Tests) is performed at least annually on the Azure DevOps environment. The PEN Test scope is determined based on Azure's DevOps areas of risk and compliance requirements. PEN Tests findings are remediated based on criticality.

Software Development

Secure Development

Azure DevOps' software development practices, across each of the feature teams, are aligned with the Microsoft SDL methodology established by CELA. The SDL methodology introduces security and privacy control specifications during the feature / component design and throughout the development process, which are reviewed through designated security roles. Azure DevOps feature teams track and complete their SDL compliance for every major and minor release of Microsoft's on-premises TFS product.

Security testing runs in parallel with release management for Azure DevOps. This is an ongoing process. For each major and minor release, security bugs identified are tracked for criticality and subsequent closure. Security fixes that are incorporated for the on-premises major and minor release are incorporated within the Azure DevOps environment as well.

A designated group of security champs within the Azure DevOps feature teams provide guidance, perform periodic security reviews, and oversee the implementation of SDL activities into Azure DevOps software development projects. The SDL process specifies testing tools to check for potential security issues, such as input / output data validation. Exceptions identified through the process must be documented and appropriately reviewed for risk and approved by Security Advisors as well as the feature team management personnel. Issues / exceptions are evaluated based on the risk and resolved or approved prior to release.

Authorized system changes are promoted from test, pre-production to production per the software change and release management process as described in the Change Management section.

Source Code Control

The Azure DevOps source code is stored within Azure DevOps' internal instance repository that provides the versioning system for the source code. Azure DevOps tracks the identity of the person who checks source code out, and what changes are made. Permission to make changes to the source code is provided by granting write access to the source code branches, which limits the access to confined project boundaries per job responsibilities. In addition, source code builds are scanned for malware prior to production release.

Access requests by Full-time Employees (FTEs) and non-FTEs to the source code repository require approval from the relevant project sponsor. Upon expiry, FTEs and non-FTEs need to submit request to the project sponsor for access renewal.

Segregation of Duties

Responsibilities for release management and production deployment are segregated among designated Azure DevOps personnel.

Change Management

Azure DevOps uses its own DevOps tools for collaboration, automated releases, and continuous delivery for delivering Azure DevOps features. From continuous integration to continuous delivery, Azure DevOps creates automated builds and repeatable workflows to keep code quality and deploy seamlessly. Azure DevOps uses its own built-in version control, and build system, and integrates releasing applications to production and operations.

Formal management responsibilities and procedures are in place to ensure reasonable control of changes to software, security or procedures. Changes are made to operational systems on a continuous basis to improve the systems with new features and bug-fixes with a valid business reason. Implemented changes require creation and retention of a “release” containing relevant information. Once released, changes are monitored for success; failed implementations are immediately rolled back and the change is not considered as completed until it is implemented and validated to operate as intended.

The Azure DevOps Change Management process is established to plan, schedule, approve, apply, distribute, and track changes to the production environment through designated responsibilities with the objective of minimizing risk and customer impact. It further controls the integrity and reliability of the environment while maintaining the pace of change required for business purposes.

Software and Infrastructure Changes

Changes within the Azure DevOps environment are categorized into software changes and infrastructure changes. Changes are tracked through production deployment as a part of the release management process, based on the type of change.

- **Software and Infrastructure Changes** - Software and infrastructure changes are modifications, enhancements and upgrades to Azure DevOps platform software and underlying infrastructure. They include release changes, hotfixes, emergency changes and configuration changes. Azure DevOps ships features on a three-week cadence. The changes are tracked and deployed using Azure DevOps Release tool. Changes submitted to the centralized repository are logged and can be traced to the individuals or system components executing them.

All activity performed, including changes made, using a user’s break-glass account is logged and alerted. Service teams will review activity to ensure any changes made were appropriate. Azure DevOps has implemented tools to perform integrity verification checks to detect unauthorized changes to software, firmware and information.

Segregation of Duties

Azure DevOps reviews the progress of feature deployment at every stage of the release pipeline with full traceability. In the Azure DevOps model, individual engineers are responsible for ensuring changes developed and implemented into the business go through impact assessment, testing, and approval processes depending on the impact of the change. In addition, the Azure DevOps feature teams are responsible for enforcing segregation of duties in the Change Management process.

Separation of Environments

Azure DevOps has implemented segregated environments for development, test and production, to support segregation of duties and prevent unauthorized changes to production. Azure DevOps maintains logical and physical separation between the DEV (development), TEST (pre-production) and PROD (production) environments. Virtual services run on different clusters in separate network segments. Access to TEST and PROD deployment boxes is restricted to authorized personnel from the Observability team.

Deployment of software to production must meet testing criteria prior to release. Production deployments use approved software builds. In addition, production data is not used or copied to non-production environments. Test scripts and synthetic data are created for use in the development and test environments.

Asset Management

Azure DevOps assets are classified in accordance with Azure DevOps Classification guidelines. The classification process is owned by the Azure DevOps SPC team. Steps are taken to protect assets commensurate with the respective asset classification.

Azure DevOps has adopted the information classification schemes used by Microsoft Corporation. Information is classified into five categories: Highly Confidential, Confidential, General, Public, and Non-business in consideration of its criticality and sensitivity of the information to Azure DevOps. Following are some examples of data elements collected by Azure DevOps features and their classification category based on the Azure DevOps Classification guidelines:

- Access Control Data (Highly Confidential)
- Customer Content (Confidential)
- End-user Identifiable Information (Confidential)
- System Metadata (Confidential)
- Organization Identifiable Information (Confidential)

The security classification level of the asset is identified based on the following factors:

- Impact on the business / process if the Confidentiality of the asset is breached
- Impact on the business / process if the Integrity of the asset is compromised
- Impact on the business / process if the Availability of the asset is not there

The level of protection is determined based on the classification of the asset. Review of asset inventory and classification is performed on a periodic basis.

Business Continuity Management

Microsoft has established an organization-wide Microsoft's Enterprise Business Continuity Methodology (EBCM) framework that serves as a guideline for developing Azure DevOps Business Continuity Program. The program includes Business Continuity Policy, Implementation Guidelines, Business Impact Analysis (BIA), Risk Assessment, Dependency Analysis, Business Continuity Plan (BCP), Incident Management Plan, and Procedures for monitoring and improving the program. The Observability team manages the Business Continuity Program for Azure DevOps.

The Disaster Recovery Plan (DRP) is intended for use by Azure DevOps Incident Managers for the recovery from high severity incidents (disasters) for Azure DevOps' critical processes. The BCP and DRP are reviewed periodically.

Azure DevOps Resiliency Program

Azure DevOps has defined the BCP to serve as a guide to respond, recover and resume operations during a serious adverse event. The BCP covers the key personnel, resources, services and actions required to continue critical business processes and operations. This plan is intended to address extended business disruptions. The development of the BCP is based on recommended guidelines of Microsoft's EBCM.

Azure DevOps' critical business processes were determined during a BIA, in which Azure DevOps estimated potential operational and financial impacts if they could not perform a process, and determined the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) of these processes.

On a periodic basis, Azure DevOps performs testing of the BCP, which is used to assess the effectiveness and usability of the BCP and to identify areas where risks can be eliminated or mitigated. The results of testing are documented, validated and approved by the appropriate personnel. This information is used to create and prioritize work items.

Capacity Management

Azure DevOps continually monitors the service to ensure availability and addresses capacity issues in a timely manner. The process for monthly capacity review is initiated by the Management team. The review includes an analysis of the capacity based on various parameters. Actions identified from the review are assigned for appropriate resolution. Additionally, the Microsoft Capacity Management team projects future capacity requirements based on internal operational reports, revenue forecasts and inputs from internal component teams.

Data Security

Please refer to the Data section above for information on data classification in Azure DevOps.

Backup of Secrets

Processes are implemented for the backup of secrets. Backup of secrets is managed by the Azure team, and is not in scope of this report.

Data Redundancy

To protect data in the case of hardware or service failures, Azure Storage geo-replicates customer data between two locations within the same region that are hundreds of miles apart; for instance, between North and West Europe or between North and South United States. The exception to this is the Brazilian datacenter which is paired with the South-Central US datacenter. For Azure blobs, customer data is replicated three times within a single datacenter and is replicated asynchronously to a second datacenter hundreds of miles away. As such, Azure always maintains the equivalent of 6 copies of customer data. This enables Azure DevOps to failover to a separate datacenter in the case of a major outage or disaster while also providing local redundancy for hardware failures within a datacenter. For Azure SQL Database, daily backups are maintained offsite by Azure to minimize data loss in the case of datacenter disasters. Backups are monitored and errors are investigated and followed-up on appropriately.

Data Location

Azure DevOps is available in [multiple geographies](#) across the world. By default, the location of Azure DevOps data is in the closest geography to the customer, but customers have the option to choose a different geography. If the customer wants to change the location, their organization's data may be migrated to a different geography, with the assistance of Microsoft support.

Data Segregation

Azure DevOps assigns each customer a unique identifier as part of the initial setup process. The mapping between the customer unique identifier and customer data location within the partition table is in a configuration database hidden from each customer. Each customer's data is segregated and partitioned within the partition database based on this unique identifier to ensure appropriate data segregation.

Customer Data Deletion

Customer data and metadata is disabled or deleted (per the direction of the customer) upon termination of their Azure DevOps Organization. Azure DevOps provides its customers with a "soft delete" period during which the organization's data can be restored. Upon termination of this "soft delete" period, the clean-up job orchestrates the delete operation among the various Azure DevOps features and processes it until completion.

Data Classification

Data (also referred to as information and assets) is classified into eleven categories, as described in the Data section above, based on how it is used or may be used within the Azure DevOps service.

Third Parties

Third parties undergo a review process through Global Procurement and an approved vendor list is established. Purchase Orders to engage a third-party require a Microsoft Master Vendor Agreement (MMVA) to be established or a review to be performed by CELA. In addition to an MMVA, a signed Non-Disclosure Agreement (NDA) is also required. Vendors requiring access to source code are required to sign a Source Code Licensing Agreement as part the vendor procurement process.

Platform Communication and Customer Secrets Protection

Data integrity is a key component of the Azure DevOps system. Customer secrets are encrypted during storage and transit. The customer facing portal and APIs only allow access to the Azure DevOps service over a secure channel.

Azure DevOps Inter-Component Communication

Internal communication between key Azure DevOps components where customer data is transmitted and involved is secured using Secure Sockets Layer (SSL). SSL certificates are Enhanced Key Usage (EKU) - enforced and self-signed, except for those certificates that are used for connections from outside the network.

Secrets Management

Azure DevOps uses Azure Key Vault for secret management. Secrets that are used to manage and maintain the service, such as SSL certificates and encryption keys, are managed, stored, and transmitted securely. Access to these secrets requires specific permission, which is logged and recorded in a secure manner. Secrets are rotated on a regular cadence and can be rotated on-demand in the case of a security event or attrition.

Cryptographic controls

Cryptographic controls and approved algorithms are used for information protection within the Azure DevOps environment, and implemented based on the Azure DevOps Cryptographic Policy and Microsoft Cryptographic Standards. Cryptographic keys are managed throughout their lifecycle (e.g., generation, distribution, revocation) in accordance with established key management processes.

Processing Integrity

Azure DevOps monitors the processing of customer transactions by collecting and analyzing the activity logs generated by the Azure DevOps system. Activity logs include commands issued by customers, their execution status, and execution metrics such as the execution time. Based on a pre-defined logic, a command is classified as:

- **Failed command** - in case the command was not able to execute completely or resulted in an error
- **Slow command** - in case the command took more than a threshold time period to execute
- **Allow list command** - a command designated out of scope for monitoring purposes, after receiving appropriate management approval

Azure DevOps feature teams analyze the trend of failed and slow commands across the Azure DevOps service using a Service Insights Dashboard to monitor the availability of the service as well as the success rate of customer transactions. Issues identified by the teams, based on the failed and slow command monitoring, or dip in the service availability below the defined SLA, are discussed during the weekly Live Site Review meetings and Monthly Service Review meetings with the leadership for investigation and remediation.

Azure DevOps performs input validation to restrict any non-permissible requests to the API which includes checking for illegal characters, misplaced whitespaces, invalid SQL escape characters etc. when receiving inputs from customers, checking for appropriateness of resources requested based on service tier, performing basic form validation, checking for validity of the user (using certificates, token, etc.), and checking for validity of account details. Based on the input parameters received from customers, Azure DevOps appropriately provisions the resources for processing of customer transactions or generates errors if the requests made are non-permissible.

System Incidents

There were no significant system incidents identified that (a) were the result of controls that were not suitably designed or operating effectively to achieve one or more of the service commitments and system requirements or otherwise (b) resulted in a significant failure in the achievement of one or more of those service commitments and system requirements during the period October 1, 2022, to September 30, 2023.

Changes to the Azure DevOps system

The only changes to the Azure DevOps system from October 1, 2022, to September 30, 2023 that would affect report users' understanding of how the system is used were the changes in in-scope features. Refer to the updated list of features in the "Report Scope and Boundary" subsection in Section III of this SOC 2 report.

Complementary User Entity Controls

The following list includes complementary user entity controls that Azure DevOps assumes its user entities have implemented. User organization auditors should determine whether the user entities have established sufficient controls in these areas:

Complementary User Entity Controls	Relevant Applicable Trust Services Criteria	Relevant Applicable C5 Criteria
Customers are responsible for reporting to Azure DevOps the incidents and alerts that are specific to their Azure DevOps accounts.	CC7.3, CC7.4, CC7.5	OIS-03, OPS-20, OPS-21, SIM-01, SIM-04, SIM-05
Customers utilizing Azure Active Directory (AAD) services are responsible for implementing appropriate authentication mechanisms and limiting administrative access to appropriate individuals to maintain integrity of their Azure DevOps account.	CC5.2, CC6.1, CC6.2, CC6.3, CC6.6	IDM-01, IDM-02, IDM-06, IDM-08, IDM-09, PSS-08, PSS-09
Customers are responsible for establishing appropriate controls over the use of their Microsoft Accounts and passwords.	CC6.1	IDM-01, IDM-02, IDM-03, IDM-06, IDM-08, IDM-09, PSS-05, PSS-08, PSS-09
Customers are responsible for reviewing the access activities associated with their Azure DevOps accounts.	CC5.2, CC6.1, CC6.2, CC6.3	IDM-01, IDM-02, IDM-03, IDM-04, IDM-05
Customers are responsible for appropriate protection of the secrets associated with their accounts.	CC6.6	IDM-08, CRY-03, CRY-04
Customers' administrators are responsible for the selection and use of their passwords.	CC6.1	IDM-01, IDM-02, IDM-03, IDM-06, IDM-08, IDM-09, PSS-05, PSS-08, PSS-09
Customers are responsible for ensuring that authorized users are added to their accounts.	CC5.2, CC6.1, CC6.2, CC6.3, CC6.6	IDM-01, IDM-02, IDM-03, IDM-04, IDM-05
Customers are responsible to implement logical access controls to provide reasonable assurance that unauthorized access to Azure DevOps projects is restricted.	CC6.1, CC6.2, CC6.6	OPS-02, IDM-01, CRY-02, PSS-04, PSS-05
Customers are responsible to assign unique IDs and secure passwords to users and customers accessing their Azure DevOps account.	CC5.2, CC6.1, CC6.2, CC6.3, CC6.6, CC6.8	IDM-01, IDM-02, IDM-03, IDM-06, IDM-08, IDM-09, PSS-05, PSS-08, PSS-09
Customers are responsible for ensuring the supervision, management and control of access to data stored in Azure DevOps.	CC5.2, CC6.1, CC6.2, CC6.3, CC6.6	IDM-01, IDM-02, IDM-03, IDM-06, IDM-08, IDM-09, PSS-05, PSS-08, PSS-09

External Subservice Organization and Complementary Subservice Organization Controls

The achievement of trust services criteria and objectives set forth in C5 related to Azure DevOps' access control, data security, vulnerability and patch management, hardware change management and network security is

dependent upon controls, known as complementary subservice organization controls that are performed by the subservice provider.

Each user entity's internal controls should be evaluated in conjunction with Azure DevOps' controls and the related tests and results described in Section IV of this report, while considering the complementary subservice organization controls expected to be implemented at the subservice organization, as described in the table, below. The scope of this report does not include controls at the external subservice organization. Through the performance of the control activities described herein, including obtaining and evaluating the SOC 2 reports for subservice provider, Azure DevOps monitors subservice provider's adherence to policies and procedures. Additionally, business process controls have been designed and implemented to identify exceptions to standard procedures and processing practices and to resolve them.

Type of Services Provided	Subservice Organization Name	Complementary Subservice Organization Controls	Relevant Applicable Trust Services Criteria	Relevant Applicable C5 Criteria
Secrets Management	Microsoft Azure	Azure is responsible for encryption and back up of secrets stored on Azure Key Vault service.	CC6.6, CC7.2, A1.2, PI1.3, PI1.5	OPS-06, OPS-07, OPS-08, OPS-09, IDM-08, CRY-03, CRY-04
Backup of SQL Database	Microsoft Azure	Azure is responsible for maintaining Point in time Restore (PITR) capabilities for the Azure DevOps data stored on Azure SQL Databases.	CC7.2, A1.2, C1.1, PI1.3, PI1.5	OPS-06, OPS-07, OPS-08, OPS-09, PSS-12
Backup of Storage Accounts	Microsoft Azure	Azure is responsible for maintaining the backup of Storage Accounts.	CC7.2, A1.2, C1.1, PI1.3, PI1.5	OPS-06, OPS-07, OPS-08, OPS-09, PSS-12
Security and anti-malware logging and vulnerability and baseline scanning	Microsoft Azure	Azure DevOps leverages Azure's logging and reporting capabilities for appropriate monitoring of security and anti-malware events and vulnerability and baseline alerts.	CC4.2, CC6.8, CC7.1, CC7.2, CC8.1	OPS-05, OPS-10, OPS-12, OPS-13, OPS-14, OPS-23, DEV-01, PSS-02, PSS-03, PSS-04
Physical and Environmental Security of Azure DevOps information	Microsoft Azure	Azure is responsible for providing physical and environmental security to Azure DevOps application and data hosted at Microsoft datacenters.	CC6.4, CC6.5, CC7.2	PS-01, PS-02, PS-03, PS-04, PS-05, PS-06, PS-07

Type of Services Provided	Subservice Organization Name	Complementary Subservice Organization Controls	Relevant Applicable Trust Services Criteria	Relevant Applicable C5 Criteria
Hardware Change Management	Microsoft Azure	Azure is responsible for hardware change management including commissioning and decommissioning.	CC6.8, CC8.1, PI1.3, PI1.4	AM-03, AM-04
Network Security of Azure DevOps	Microsoft Azure	Azure is responsible for maintaining controls over protection of the network environment and infrastructure, including perimeter firewalls and restricting access to network devices.	CC6.4, CC6.5, CC7.2	COS-01, COS-02, COS-03, COS-04, COS-05, COS-06, COS-07, COS-08

Section IV:
Management of Microsoft's
Description of its Relevant
Criteria and Objectives and
Related Controls, and
Independent Service Auditor's
Description of Tests of
Controls and Results

Section IV: Management of Microsoft's Description of its Relevant Criteria and Objectives and Related Controls, and Independent Service Auditor's Description of Tests of Controls and Results

Description of testing procedures performed

Deloitte & Touche LLP performed a variety of tests relating to the controls listed in this section throughout the period from October 1, 2022 through September 30, 2023. Our tests of controls were performed on controls as they existed during the period of October 1, 2022 through September 30, 2023 and were applied to those controls specified by Microsoft.

In determining the nature, timing, and extent of tests, we considered (a) the nature and frequency of the controls being tested, (b) the types of available evidential matter, (c) the assessed level of control risk, (d) the expected effectiveness of the test, and (e) our understanding of the control environment.

In addition to the tests listed below, ascertained through multiple inquiries with management and the control owner that each control activity listed below operated as described throughout the period. Tests performed are described below:

Test	Description
Corroborative inquiry	Conducted detailed interviews with relevant personnel to obtain evidence that the control was in operation during the report period and is accompanied by other procedures noted below that are necessary to corroborate the information derived from the inquiry.
Observation	Observed the performance of the control during the report period to evidence application of the specific control activity.
Examination of documentation/inspection	If the performance of the control is documented, inspected documents and reports indicating performance of the control.
Reperformance of monitoring activities or manual controls	Obtained documents used in the monitoring activity or manual control activity and independently reperformed the procedures. Compared any exception items identified with those identified by the responsible control owner.
Reperformance of programmed processing	Input test data, manually calculated expected results, and compared actual results of processing to expectations.

Reliability of information produced by the Service Organization

We performed procedures to evaluate whether the information provided by the service organization, which includes (a) information in response to ad hoc requests from the service auditor (e.g., population lists), and (b) information used in the execution of a control (e.g., exception reports or transaction reconciliations), was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

Our procedures to evaluate whether this information was sufficiently reliable included obtaining evidence regarding the accuracy and completeness included procedures to address (a) the accuracy and completeness of source data, and (b) the creation and modification of applicable report logic and parameters. While these procedures were not specifically called out in the test procedures listed in this section, they were completed as a component of our testing to support the evaluation of whether or not the information is sufficiently precise and detailed for purposes of fully testing the controls identified by the Service Organization.

Reporting on results of testing

The concept of materiality is not applied when reporting the results of control tests because Deloitte & Touche LLP does not have the ability to determine whether an exception will be relevant to a particular user entity. Consequently, Deloitte & Touche LLP reports all exceptions.

Results of Testing Performed

The information regarding the tests of operating effectiveness is explained below in Three parts:

Part A: Contains the Trust Services Criteria, the related Azure DevOps' control activities that cover those criteria, and the results of the test procedures performed.

Part B: Contains the objectives set forth in C5, the related control activities that cover those objectives, and the results of the test procedures performed.

Part C: Contains the details of the test procedures performed to test the operating effectiveness of the Azure DevOps' control activities and the results of the testing performed.

The applicable trust services criteria, the objectives set forth in C5, and Azure DevOps' control activities in Part A, B and C are provided by Azure DevOps.

Part A: Trust Services Criteria, Control Activities provided by Azure DevOps, and Test Results provided by Deloitte & Touche LLP

CONTROL ENVIRONMENT

Trust Criteria	Azure DevOps Activity	Test Result
CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	<p>SOC2 - 8. Microsoft has defined disciplinary actions for employees and contingent staff that commit a security breach or violate the security policy.</p> <p>SOC2 - 9. Microsoft personnel and contingent staff undergo formal screening, including background verification checks as a part of the hiring process prior to being granted access. Additional screening is conducted in accordance with customer specific requirements, for employees with access to applicable data.</p> <p>SOC2 - 10. Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees must acknowledge Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage.</p> <p>ELC - 1. Microsoft's values are accessible to employees via the Values SharePoint site and are updated as necessary by management.</p> <p>ELC - 2. Microsoft Compliance and Ethics team updates the Standards of Business Conduct (SBC) as necessary and the Code is made available internally and externally. The SBC reflects Microsoft's continued commitment to ethical business practices and regulatory compliance. Compliance and Ethics team provides an annual Standards of Business Conduct training course that is mandatory for all employees. Employees who do not complete the training on time are tracked and followed up with appropriately.</p> <p>ELC - 3. Microsoft maintains several mechanisms (email, phone, fax, website) that permit employees and non-employees to</p>	No exceptions noted.

Trust Criteria	Azure DevOps Activity	Test Result
	communicate confidential and / or anonymous reports concerning Business Conduct.	
CC1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	<p>ELC - 4. The Audit Committee (AC) reviews its Charter and Responsibilities as listed in its calendar on an annual basis. The AC Responsibilities include meeting with the external and internal auditors on a quarterly basis; providing oversight on the development and performance of controls; and completing an annual self-evaluation.</p> <p>ELC - 5. Internal Audit Charter directs Internal Audit to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment.</p>	No exceptions noted.
CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	<p>IS - 1. Microsoft has documented and communicated a security policy that defines the information security rules and requirements for the Azure DevOps environment.</p> <p>IS - 3. Management has established defined roles and responsibilities to oversee implementation of the information security policy across the service.</p> <p>SOC2 - 14. Microsoft manages a compliance program with representation from various cross-functional teams including CELA, Marketing, security champions to identify and manage compliance with relevant statutory, regulatory and contractual requirements.</p> <p>ELC - 5. Internal Audit Charter directs Internal Audit to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment.</p>	No exceptions noted.

Trust Criteria	Azure DevOps Activity	Test Result
<p>CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.</p>	<p>IS - 4. An information security education and awareness program is established that includes policy training and periodic security updates to Azure DevOps personnel.</p> <p>SOC2 - 9. Microsoft personnel and contingent staff undergo formal screening, including background verification checks as a part of the hiring process prior to being granted access. Additional screening is conducted in accordance with customer specific requirements, for employees with access to applicable data.</p> <p>SOC2 - 10. Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees must acknowledge Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage.</p> <p>ELC - 1. Microsoft's values are accessible to employees via the Values SharePoint site and are updated as necessary by management.</p> <p>ELC - 7. Employees hold periodic connects with their managers to validate they are on the expected career path and facilitate greater collaboration. Employees also review their performance against their documented deliverables (priorities) and discuss the results with their managers.</p> <p>ELC - 8. The Compensation Committee is responsible for reviewing and discussing plans for executive officer development and corporate succession plans for the CEO and other executive officers.</p>	<p>No exceptions noted.</p>
<p>CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.</p>	<p>IS - 2. The security policy is reviewed and approved annually by Microsoft management.</p> <p>IS - 3. Management has established defined roles and responsibilities to oversee implementation of the information security policy across the service.</p>	<p>No exceptions noted.</p>

Trust Criteria	Azure DevOps Activity	Test Result
	<p>SOC2 - 8. Microsoft has defined disciplinary actions for employees and contingent staff that commit a security breach or violate the security policy.</p> <p>SOC2 - 10. Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees must acknowledge Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage.</p> <p>SOC2 - 15. Microsoft performs annual Information Security Management System (ISMS) review and results are reviewed with management. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.</p> <p>ELC - 2. Microsoft Compliance and Ethics team updates the Standards of Business Conduct (SBC) as necessary and the Code is made available internally and externally. The SBC reflects Microsoft's continued commitment to ethical business practices and regulatory compliance. Compliance and Ethics team provides an annual Standards of Business Conduct training course that is mandatory for all employees. Employees who do not complete the training on time are tracked and followed up with appropriately.</p> <p>ELC - 3. Microsoft maintains several mechanisms (email, phone, fax, website) that permit employees and non-employees to communicate confidential and / or anonymous reports concerning Business Conduct.</p> <p>ELC - 7. Employees hold periodic connects with their managers to validate they are on the expected career path and facilitate greater collaboration. Employees also review their performance against their documented deliverables (priorities) and discuss the results with their managers.</p>	

COMMUNICATION AND INFORMATION

Trust Criteria	Azure DevOps Activity	Test Result
<p>CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.</p>	<p>IS - 1. Microsoft has documented and communicated a security policy that defines the information security rules and requirements for the Azure DevOps environment.</p> <p>SOC2 - 13. Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization.</p> <p>SOC2 - 14. Microsoft manages a compliance program with representation from various cross-functional teams including CELA, Marketing, security champions to identify and manage compliance with relevant statutory, regulatory and contractual requirements.</p> <p>SOC2 - 15. Microsoft performs annual Information Security Management System (ISMS) review and results are reviewed with management. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.</p> <p>BC - 1. Management conducts a risk assessment to identify and assess continuity risks related to Azure DevOps. The Business Impact Analysis is carried out and impacts are assessed for critical services based on revenue and operations considerations.</p> <p>ELC - 5. Internal Audit Charter directs Internal Audit to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment.</p> <p>ELC - 9. The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed</p>	<p>No exceptions noted.</p>

Trust Criteria	Azure DevOps Activity	Test Result
	bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management.	
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	<p>IS - 1. Microsoft has documented and communicated a security policy that defines the information security rules and requirements for the Azure DevOps environment.</p> <p>IS - 3. Management has established defined roles and responsibilities to oversee implementation of the information security policy across the service.</p> <p>IS - 4. An information security education and awareness program is established that includes policy training and periodic security updates to Azure DevOps personnel.</p> <p>SOC2 - 3. The service maintains a customer support website that describes the process for customers and other external users to inform about potential security issues and submitting complaints. Reported issues are reviewed and addressed per documented incident management procedures.</p> <p>SOC2 - 4. The service maintains and communicates the confidentiality and related security obligations for customer data via the Microsoft Trust Center. Guidelines and recommendations for the secure use of the cloud services, as applicable, are communicated to customers.</p> <p>SOC2 - 6. The service maintains and notifies customers of potential changes, and security and availability type of events that may impact the service, through an online Service Dashboard. Changes to the security commitments and security obligations of the service's customers are updated on the Azure DevOps website in a timely manner.</p> <p>SOC2 - 7. Prior to engaging in service, customers are required to review and agree with the acceptable use of data and the Service, as well as security and privacy requirements, which are defined in the Microsoft Online Services Use Rights, Microsoft Online Subscription</p>	No exceptions noted.

Trust Criteria	Azure DevOps Activity	Test Result
	<p>Agreement, Privacy Statement and Technical Overview of the Security Features.</p> <p>SOC2 - 10. Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees must acknowledge Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage.</p> <p>SOC2 - 14. Microsoft manages a compliance program with representation from various cross-functional teams including CELA, Marketing, security champions to identify and manage compliance with relevant statutory, regulatory and contractual requirements.</p> <p>IM - 1. An incident management framework is established and communicated with defined processes, roles and responsibilities for the detection, escalation and response of incidents.</p> <p>IM - 3. The Service Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures.</p> <p>ELC - 2. Microsoft Compliance and Ethics team updates the Standards of Business Conduct (SBC) as necessary and the Code is made available internally and externally. The SBC reflects Microsoft's continued commitment to ethical business practices and regulatory compliance. Compliance and Ethics team provides an annual Standards of Business Conduct training course that is mandatory for all employees. Employees who do not complete the training on time are tracked and followed up with appropriately.</p> <p>ELC - 3. Microsoft maintains several mechanisms (email, phone, fax, website) that permit employees and non-employees to communicate confidential and / or anonymous reports concerning Business Conduct.</p>	

Trust Criteria	Azure DevOps Activity	Test Result
CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	<p>IS - 1. Microsoft has documented and communicated a security policy that defines the information security rules and requirements for the Azure DevOps environment.</p> <p>IS - 3. Management has established defined roles and responsibilities to oversee implementation of the information security policy across the service.</p> <p>IS - 4. An information security education and awareness program is established that includes policy training and periodic security updates to Azure DevOps personnel.</p> <p>SOC2 - 3. The service maintains a customer support website that describes the process for customers and other external users to inform about potential security issues and submitting complaints. Reported issues are reviewed and addressed per documented incident management procedures.</p> <p>SOC2 - 4. The service maintains and communicates the confidentiality and related security obligations for customer data via the Microsoft Trust Center. Guidelines and recommendations for the secure use of the cloud services, as applicable, are communicated to customers.</p> <p>SOC2 - 5. The service maintains and distributes an accurate system description to authorized users.</p> <p>SOC2 - 6. The service maintains and notifies customers of potential changes, and security and availability type of events that may impact the service, through an online Service Dashboard. Changes to the security commitments and security obligations of the service's customers are updated on the Azure DevOps website in a timely manner.</p> <p>SOC2 - 7. Prior to engaging in service, customers are required to review and agree with the acceptable use of data and the Service, as well as security and privacy requirements, which are defined in the Microsoft Online Services Use Rights, Microsoft Online Subscription</p>	No exceptions noted.

Trust Criteria	Azure DevOps Activity	Test Result
	<p>Agreement, Privacy Statement and Technical Overview of the Security Features.</p> <p>SOC2 - 10. Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees must acknowledge Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage.</p> <p>SOC2 - 14. Microsoft manages a compliance program with representation from various cross-functional teams including CELA, Marketing, security champions to identify and manage compliance with relevant statutory, regulatory and contractual requirements.</p> <p>SOC2 - 15. Microsoft performs annual Information Security Management System (ISMS) review and results are reviewed with management. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.</p> <p>IM - 1. An incident management framework is established and communicated with defined processes, roles and responsibilities for the detection, escalation and response of incidents.</p> <p>IM - 3. The Service Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures.</p> <p>ELC - 2. Microsoft Compliance and Ethics team updates the Standards of Business Conduct (SBC) as necessary and the Code is made available internally and externally. The SBC reflects Microsoft's continued commitment to ethical business practices and regulatory compliance. Compliance and Ethics team provides an annual Standards of Business Conduct training course that is mandatory for all employees. Employees who do not complete the training on time are tracked and followed up with appropriately.</p>	

Trust Criteria	Azure DevOps Activity	Test Result
	ELC - 3. Microsoft maintains several mechanisms (email, phone, fax, website) that permit employees and non-employees to communicate confidential and / or anonymous reports concerning Business Conduct.	

RISK ASSESSMENT

Trust Criteria	Azure DevOps Activity	Test Result
CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	<p>SOC2 - 4. The service maintains and communicates the confidentiality and related security obligations for customer data via the Microsoft Trust Center. Guidelines and recommendations for the secure use of the cloud services, as applicable, are communicated to customers.</p> <p>SOC2 - 6. The service maintains and notifies customers of potential changes, and security and availability type of events that may impact the service, through an online Service Dashboard. Changes to the security commitments and security obligations of the service's customers are updated on the Azure DevOps website in a timely manner.</p> <p>SOC2 - 13. Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization.</p> <p>SOC2 - 14. Microsoft manages a compliance program with representation from various cross-functional teams including CELA, Marketing, security champions to identify and manage compliance with relevant statutory, regulatory and contractual requirements.</p>	No exceptions noted.

Trust Criteria	Azure DevOps Activity	Test Result
	<p>SOC2 - 15. Microsoft performs annual Information Security Management System (ISMS) review and results are reviewed with management.</p> <p>This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.</p> <p>SOC2 - 17. Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within Azure DevOps environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Legal and Corporate Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements.</p> <p>SOC2 - 18. Microsoft Azure DevOps performs an annual risk assessment that covers security, continuity, and operational risks. As part of this process, threats to security are identified and risks from these threats are formally assessed.</p> <p>BC - 1. Management conducts a risk assessment to identify and assess continuity risks related to Azure DevOps. The Business Impact Analysis is carried out and impacts are assessed for critical services based on revenue and operations considerations.</p> <p>ELC - 5. Internal Audit Charter directs Internal Audit to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment.</p> <p>ELC - 9. The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management.</p>	

Trust Criteria	Azure DevOps Activity	Test Result
<p>CC3.2 COSO Principle 7: 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.</p>	<p>VM - 1. Production and supporting infrastructure are configured to log and collect security events.</p> <p>VM - 2. Administrator activity is logged.</p> <p>VM - 3. A monitoring system is implemented on production and supporting infrastructure to monitor the service for potential malicious activity and intrusion past service trust boundaries.</p> <p>VM - 6. Procedures are established to monitor production and supporting infrastructure for known security vulnerabilities. Identified security vulnerabilities are remediated.</p> <p>VM - 7. The availability of the service is monitored through third-party and internal tools, and the status is communicated through a Service Dashboard.</p> <p>IM - 1. An incident management framework is established and communicated with defined processes, roles and responsibilities for the detection, escalation and response of incidents.</p> <p>BC - 1. Management conducts a risk assessment to identify and assess continuity risks related to Azure DevOps. The Business Impact Analysis is carried out and impacts are assessed for critical services based on revenue and operations considerations.</p> <p>SOC2 - 12. The security baselines are refreshed for Azure DevOps on a periodic basis.</p> <p>SOC2 - 15. Microsoft performs annual Information Security Management System (ISMS) review and results are reviewed with management.</p> <p>This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.</p> <p>SOC2 - 17. Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed</p>	<p>No exceptions noted.</p>

Trust Criteria	Azure DevOps Activity	Test Result
	<p>within Azure DevOps environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Legal and Corporate Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements.</p> <p>ELC - 5. Internal Audit Charter directs Internal Audit to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment.</p> <p>ELC - 9. The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management.</p> <p>C5 -12. Management has developed and documented a risk assessment policy to address the purpose, scope, roles, responsibilities for managing deviations from the security policies/standards. The risk assessment policy and procedures are reviewed and updated on an annual basis.</p>	
CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	<p>VM - 1. Production and supporting infrastructure are configured to log and collect security events.</p> <p>VM - 2. Administrator activity is logged.</p> <p>VM - 3. A monitoring system is implemented on production and supporting infrastructure to monitor the service for potential malicious activity and intrusion past service trust boundaries.</p> <p>VM - 6. Procedures are established to monitor production and supporting infrastructure for known security vulnerabilities. Identified security vulnerabilities are remediated.</p>	No exceptions noted.

Trust Criteria	Azure DevOps Activity	Test Result
	<p>VM - 7. The availability of the service is monitored through third-party and internal tools, and the status is communicated through a Service Dashboard.</p> <p>IM - 1. An incident management framework is established and communicated with defined processes, roles and responsibilities for the detection, escalation and response of incidents.</p> <p>BC - 1. Management conducts a risk assessment to identify and assess continuity risks related to Azure DevOps. The Business Impact Analysis is carried out and impacts are assessed for critical services based on revenue and operations considerations.</p> <p>SOC2 - 2. The service maintains an inventory of key information assets. Procedures are established to review usage of key information assets on at least an annual basis.</p> <p>SOC2 - 12. The security baselines are refreshed for Azure DevOps on a periodic basis.</p> <p>SOC2 - 15. Microsoft performs annual Information Security Management System (ISMS) review and results are reviewed with management.</p> <p>This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.</p> <p>SOC2 - 17. Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within Azure DevOps environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Legal and Corporate Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements.</p> <p>ELC - 9. The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed</p>	

Trust Criteria	Azure DevOps Activity	Test Result
	bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management.	
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	<p>SOC2 - 13. Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization.</p> <p>SOC2 - 14. Microsoft manages a compliance program with representation from various cross-functional teams including CELA, Marketing, security champions to identify and manage compliance with relevant statutory, regulatory and contractual requirements.</p> <p>SOC2 - 15. Microsoft performs annual Information Security Management System (ISMS) review and results are reviewed with management.</p> <p>This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.</p> <p>SOC2 - 17. Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within Azure DevOps environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Legal and Corporate Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements.</p> <p>BC - 1. Management conducts a risk assessment to identify and assess continuity risks related to Azure DevOps. The Business Impact Analysis is carried out and impacts are assessed for critical services based on revenue and operations considerations.</p> <p>ELC - 5. Internal Audit Charter directs Internal Audit to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately</p>	No exceptions noted.

Trust Criteria	Azure DevOps Activity	Test Result
	<p>addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment.</p> <p>ELC - 8. The Compensation Committee is responsible for reviewing and discussing plans for executive officer development and corporate succession plans for the CEO and other executive officers.</p> <p>ELC - 9. The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management.</p> <p>C5 - 12. Management has developed and documented a risk assessment policy to address the purpose, scope, roles, responsibilities for managing deviations from the security policies/standards. The risk assessment policy and procedures are reviewed and updated on an annual basis.</p>	

MONITORING ACTIVITIES

Trust Criteria	Azure DevOps Activity	Test Result
CC4.1 COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	<p>VM - 3. A monitoring system is implemented on production and supporting infrastructure to monitor the service for potential malicious activity and intrusion past service trust boundaries.</p> <p>VM - 4. Procedures have been established to investigate and respond to the malicious events detected by the monitoring system for timely resolution.</p>	No exceptions noted.

Trust Criteria	Azure DevOps Activity	Test Result
	<p>VM - 6. Procedures are established to monitor production and supporting infrastructure for known security vulnerabilities. Identified security vulnerabilities are remediated.</p> <p>VM - 8. Penetration testing is performed on critical infrastructure components at least annually. Findings are documented, tracked and remediated.</p> <p>VM - 9. Azure DevOps provides logging mechanisms that can be configured by customers to log activities and metrics.</p> <p>IM - 1. An incident management framework is established and communicated with defined processes, roles and responsibilities for the detection, escalation and response of incidents.</p> <p>IM - 2. Events, thresholds and metrics are defined and configured to detect incidents and alert the associated Service Operations team.</p> <p>IM - 3. The Service Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures.</p> <p>SOC2 - 12. The security baselines are refreshed for Azure DevOps on a periodic basis.</p> <p>SOC2 - 15. Microsoft performs annual Information Security Management System (ISMS) review and results are reviewed with management.</p> <p>This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.</p> <p>SOC2 - 19. Microsoft Azure DevOps undergoes independent audits and assessments, at least annually, to monitor and verify compliance with security requirements. Findings are recorded, reviewed, prioritized, and remediation plans are developed.</p> <p>BC - 1. Management conducts a risk assessment to identify and assess continuity risks related to Azure DevOps. The Business</p>	

Trust Criteria	Azure DevOps Activity	Test Result
	<p>Impact Analysis is carried out and impacts are assessed for critical services based on revenue and operations considerations.</p> <p>ELC - 5. Internal Audit Charter directs Internal Audit to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment.</p> <p>ELC - 9. The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management.</p>	
<p>CC4.2 COSO Principle 17: 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.</p>	<p>VM - 3. A monitoring system is implemented on production and supporting infrastructure to monitor the service for potential malicious activity and intrusion past service trust boundaries.</p> <p>VM - 4. Procedures have been established to investigate and respond to the malicious events detected by the monitoring system for timely resolution.</p> <p>VM - 6. Procedures are established to monitor production and supporting infrastructure for known security vulnerabilities. Identified security vulnerabilities are remediated.</p> <p>IM - 1. An incident management framework is established and communicated with defined processes, roles and responsibilities for the detection, escalation and response of incidents.</p> <p>IM - 2. Events, thresholds and metrics are defined and configured to detect incidents and alert the associated Service Operations team.</p> <p>IM - 3. The Service Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures.</p>	No exceptions noted.

Trust Criteria	Azure DevOps Activity	Test Result
	<p>SOC2 - 12. The security baselines are refreshed for Azure DevOps on a periodic basis.</p> <p>SOC2 - 15. Microsoft performs annual Information Security Management System (ISMS) review and results are reviewed with management.</p> <p>This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.</p> <p>BC - 1. Management conducts a risk assessment to identify and assess continuity risks related to Azure DevOps. The Business Impact Analysis is carried out and impacts are assessed for critical services based on revenue and operations considerations.</p> <p>ELC - 4. The Audit Committee (AC) reviews its Charter and Responsibilities as listed in its calendar on an annual basis. The AC Responsibilities include meeting with the external and internal auditors on a quarterly basis; providing oversight on the development and performance of controls; and completing an annual self-evaluation.</p> <p>ELC - 5. Internal Audit Charter directs Internal Audit to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment.</p> <p>C5 - 12. Management has developed and documented a risk assessment policy to address the purpose, scope, roles, responsibilities for managing deviations from the security policies/standards. The risk assessment policy and procedures are reviewed and updated on an annual basis.</p>	

CONTROL ACTIVITIES

Trust Criteria	Azure DevOps Activity	Test Result
CC5.1 COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	<p>BC - 2. Business Continuity Plans (BCP) are documented and published for critical services, which provide roles and responsibilities and detailed procedures for recovery and reconstitution of systems to a known state per defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Plans are reviewed on an annual basis, at a minimum.</p> <p>SOC2 - 13. Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization.</p> <p>SOC2 - 15. Microsoft performs annual Information Security Management System (ISMS) review and results are reviewed with management.</p> <p>This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.</p> <p>SOC2 - 17. Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within Azure DevOps environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Legal and Corporate Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements.</p> <p>SDL - 3. Responsibilities for production deployment are segregated within the feature teams.</p> <p>CM - 3. Responsibilities for approving and implementing changes to the features are segregated among designated personnel.</p>	No exceptions noted.

Trust Criteria	Azure DevOps Activity	Test Result
	<p>CM - 6. Any changes to production via break-glass have been reviewed to ensure all changes were appropriate.</p> <p>ELC - 5. Internal Audit Charter directs Internal Audit to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment.</p> <p>ELC - 9. The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management.</p>	
CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	<p>BC - 2. Business Continuity Plans (BCP) are documented and published for critical services, which provide roles and responsibilities and detailed procedures for recovery and reconstitution of systems to a known state per defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Plans are reviewed on an annual basis, at a minimum.</p> <p>SOC2 - 13. Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization.</p> <p>SOC2 - 15. Microsoft performs annual Information Security Management System (ISMS) review and results are reviewed with management.</p> <p>This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.</p> <p>SOC2 - 17. Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed</p>	No exceptions noted.

Trust Criteria	Azure DevOps Activity	Test Result
	<p>within Azure DevOps environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Legal and Corporate Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements.</p> <p>SDL - 1. Development of new features and changes to existing features follow a defined approach based on the Microsoft Secure Development Lifecycle (SDL) methodology.</p> <p>SDL - 2. Applicable operational security and internal control requirements are documented and approved for Azure DevOps.</p> <p>OA - 1. Administrative access to the service is controlled through defined interfaces that require authentication using AD credentials.</p> <p>OA - 2. Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning access to employees, contractors, and service providers to specific applications or information resources.</p> <p>OA - 3. Procedures are in place to disable accounts on a timely basis, upon the user's termination.</p> <p>OA - 5. Access privileges are reviewed quarterly to determine if access rights are commensurate to the user's job duties. Access is modified based on the results of the reviews.</p> <p>OA - 6. Procedures are established for granting temporary access for personnel to customer data and applications upon appropriate approval.</p> <p>OA - 8. Alerts are generated when a break-glass account is used to access production environment.</p> <p>OA - 10. Access to production resources requires the use of a Secure Admin Workstation (SAW) which requires MFA for access. SAWs are hardened and secured devices with restricted access.</p>	

Trust Criteria	Azure DevOps Activity	Test Result
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	<p>IS - 1. Microsoft has documented and communicated a security policy that defines the information security rules and requirements for the Azure DevOps environment.</p> <p>IS - 2. The security policy is reviewed and approved annually by Microsoft management.</p> <p>IS - 3. Management has established defined roles and responsibilities to oversee implementation of the information security policy across the service.</p> <p>IS - 4. An information security education and awareness program is established that includes policy training and periodic security updates to Azure DevOps personnel.</p> <p>IM - 3. The Service Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures.</p> <p>VM - 4. Procedures have been established to investigate and respond to the malicious events detected by the monitoring system for timely resolution.</p> <p>ELC - 2. Microsoft Compliance and Ethics team updates the Standards of Business Conduct (SBC) as necessary and the Code is made available internally and externally. The SBC reflects Microsoft's continued commitment to ethical business practices and regulatory compliance. Compliance and Ethics team provides an annual Standards of Business Conduct training course that is mandatory for all employees. Employees who do not complete the training on time are tracked and followed up with appropriately.</p> <p>ELC - 3. Microsoft maintains several mechanisms (email, phone, fax, website) that permit employees and non-employees to communicate confidential and / or anonymous reports concerning Business Conduct.</p> <p>ELC - 5. Internal Audit Charter directs Internal Audit to provide independent and objective audit, investigative, and advisory</p>	No exceptions noted.

Trust Criteria	Azure DevOps Activity	Test Result
	<p>services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment.</p> <p>ELC - 7. Employees hold periodic connects with their managers to validate they are on the expected career path and facilitate greater collaboration. Employees also review their performance against their documented deliverables (priorities) and discuss the results with their managers.</p>	

LOGICAL AND PHYSICAL ACCESS CONTROLS

Trust Criteria	Azure DevOps Activity	Test Result
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.	<p>OA - 1. Administrative access to the service is controlled through defined interfaces that require authentication using AD credentials.</p> <p>OA - 2. Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning access to employees, contractors, and service providers to specific applications or information resources.</p> <p>OA - 3. Procedures are in place to disable accounts on a timely basis, upon the user's termination.</p> <p>OA - 4. Password complexity standards are defined and enforced for Azure DevOps personnel credentials.</p> <p>OA - 5. Access privileges are reviewed quarterly to determine if access rights are commensurate to the user's job duties. Access is modified based on the results of the reviews.</p> <p>OA - 6. Procedures are established for granting temporary access for personnel to customer data and applications upon appropriate approval.</p> <p>OA - 7. Authentication over an encrypted Remote Desktop Connection is used for administrator access to the production environment.</p> <p>OA - 8. Alerts are generated when a break-glass account is used to access a production environment.</p> <p>OA - 9. Production domain-level user accounts are disabled after a stipulated period of inactivity.</p> <p>OA - 10. Access to production resources requires the use of a Secure Admin Workstation (SAW) which requires MFA for access. SAWs are hardened and secured devices with restricted access.</p> <p>LA - 1. External access to customer data stored in the service requires authentication.</p>	No exceptions noted.

Trust Criteria	Azure DevOps Activity	Test Result
	<p>LA - 2. Customer credentials used to access the service meet the applicable password policy requirements.</p> <p>LA - 3. Logical segregation is implemented to restrict unauthorized access to other customer tenants.</p> <p>LA - 4. Customer data that is confidential is protected while in storage within the service.</p> <p>LA - 5. Customer-configured authorization settings can be set to further restrict authentication methods.</p> <p>LA - 6. User sessions within the service portal expire after a stipulated period of inactivity.</p> <p>DS - 3. Internal communication between key components where customer data is transmitted / involved is secured using SSL or equivalent mechanism(s).</p> <p>DS - 8. Upon termination of a customer account, the customer data is removed based upon the stipulated retention and removal timelines.</p> <p>SOC2 - 1. Service assets are classified in accordance with Microsoft Online Services Classification Guidelines. Microsoft has conducted security categorization for its information and information systems and the results are documented, reviewed and approved by the authorizing official.</p> <p>SOC2 - 2. The service maintains an inventory of key information assets. Procedures are established to review usage of key information assets on at least an annual basis.</p>	
CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system	<p>OA - 1. Administrative access to the service is controlled through defined interfaces that require authentication using AD credentials.</p> <p>OA - 2. Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning access to</p>	No exceptions noted.

Trust Criteria	Azure DevOps Activity	Test Result
credentials are removed when user access is no longer authorized.	<p>employees, contractors, and service providers to specific applications or information resources.</p> <p>OA - 3. Procedures are in place to disable accounts on a timely basis, upon the user's termination.</p> <p>OA - 5. Access privileges are reviewed quarterly to determine if access rights are commensurate to the user's job duties. Access is modified based on the results of the reviews.</p> <p>OA - 6. Procedures are established for granting temporary access for personnel to customer data and applications upon appropriate approval.</p> <p>OA - 8. Alerts are generated when a break-glass account is used to access production environment.</p> <p>OA - 9. Production domain-level user accounts are disabled after a stipulated period of inactivity.</p> <p>OA - 10. Access to production resources requires the use of a Secure Admin Workstation (SAW) which requires MFA for access. SAWs are hardened and secured devices with restricted access.</p> <p>LA - 1. External access to customer data stored in the service requires authentication.</p> <p>LA - 5. Customer-configured authorization settings can be set to further restrict authentication methods.</p> <p>LA - 6. User sessions within the service portal expire after a stipulated period of inactivity.</p>	
CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and	<p>OA - 1. Administrative access to the service is controlled through defined interfaces that require authentication using AD credentials.</p> <p>OA - 2. Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning access to employees, contractors, and service providers to specific applications or information resources.</p>	No exceptions noted.

Trust Criteria	Azure DevOps Activity	Test Result
segregation of duties, to meet the entity's objectives.	<p>OA - 3. Procedures are in place to disable accounts on a timely basis, upon the user's termination.</p> <p>OA - 5. Access privileges are reviewed quarterly to determine if access rights are commensurate to the user's job duties. Access is modified based on the results of the reviews.</p> <p>OA - 6. Procedures are established for granting temporary access for personnel to customer data and applications upon appropriate approval.</p> <p>OA - 8. Alerts are generated when a break-glass account is used to access a production environment.</p> <p>OA - 9. Production domain-level user accounts are disabled after a stipulated period of inactivity.</p> <p>OA - 10. Access to production resources requires the use of a Secure Admin Workstation (SAW) which requires MFA for access. SAWs are hardened and secured devices with restricted access.</p> <p>LA - 6. User sessions within the service portal expire after a stipulated period of inactivity.</p>	
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.	<p>This Trust Service criteria is not applicable to Azure DevOps due to the following reasons:</p> <p>The Physical and Environmental (PE) controls are performed by Microsoft Azure which, as mentioned in the system description, is carved out within the Azure DevOps SOC 2 report.</p> <p>Azure DevOps does not own, operate or manage PE controls and criteria anticipated by this AICPA trust criteria.</p>	No exceptions noted.
CC6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been	<p>This Trust Service criteria is not applicable to Azure DevOps due to the following reasons:</p>	No exceptions noted.

Trust Criteria	Azure DevOps Activity	Test Result
diminished and is no longer required to meet the entity's objectives.	<p>The Physical and Environmental (PE) controls are performed by Microsoft Azure which, as mentioned in the system description, is carved out within the Azure DevOps SOC 2 report.</p> <p>Azure DevOps does not own, operate or manage PE controls and criteria anticipated by this AICPA trust criteria.</p>	
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	<p>LA - 1. External access to customer data stored in the service requires authentication.</p> <p>LA - 3. Logical segregation is implemented to restrict unauthorized access to other customer tenants.</p> <p>LA - 5. Customer-configured authorization settings can be set to further restrict authentication methods.</p> <p>DS - 1. Cryptographic certificates, keys, and customer access keys used for communication between the features and other internal components are stored securely and are rotated on a periodic basis.</p> <p>DS - 2. Customer data communicated through service interfaces is encrypted during transmission over external networks.</p> <p>DS - 3. Internal communication between key components where customer data is transmitted / involved is secured using SSL or equivalent mechanism(s).</p> <p>DS - 4. Cryptographic controls are used for information protection within the platform based on the Cryptographic Policy and Key Management procedures.</p> <p>OA - 1. Administrative access to the service is controlled through defined interfaces that require authentication using AD credentials.</p> <p>OA - 7. Authentication over an encrypted Remote Desktop Connection is used for administrator access to the production environment.</p> <p>PI - 3. Azure DevOps performs input validation to restrict any non-permissible requests to the API.</p>	No exceptions noted.

Trust Criteria	Azure DevOps Activity	Test Result
CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	<p>DS - 2. Customer data communicated through service interfaces is encrypted during transmission over external networks.</p> <p>DS - 3. Internal communication between key components where customer data is transmitted / involved is secured using SSL or equivalent mechanism(s).</p> <p>DS - 4. Cryptographic controls are used for information protection within the platform based on the Cryptographic Policy and Key Management procedures.</p> <p>OA - 7. Authentication over an encrypted Remote Desktop Connection is used for administrator access to the production environment.</p>	No exceptions noted.
CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	<p>VM - 1. Production and supporting infrastructure are configured to log and collect security events.</p> <p>VM - 2. Administrator activity is logged.</p> <p>VM - 3. A monitoring system is implemented on production and supporting infrastructure to monitor the service for potential malicious activity and intrusion past service trust boundaries.</p> <p>VM - 4. Procedures have been established to investigate and respond to the malicious events detected by the monitoring system for timely resolution.</p> <p>VM - 5. Procedures are established to evaluate and implement Microsoft released patches to service components.</p> <p>VM - 6. Procedures are established to monitor production and supporting infrastructure for known security vulnerabilities. Identified security vulnerabilities are remediated.</p> <p>VM - 7. The availability of the service is monitored through third-party and internal tools, and the status is communicated through a Service Dashboard.</p>	No exceptions noted.

Trust Criteria	Azure DevOps Activity	Test Result
	<p>OA - 1. Administrative access to the service is controlled through defined interfaces that require authentication using AD credentials.</p> <p>OA - 2. Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning access to employees, contractors, and service providers to specific applications or information resources.</p> <p>OA - 8. Alerts are generated when a break-glass account is used to access production environment.</p> <p>IM - 1. An incident management framework is established and communicated with defined processes, roles and responsibilities for the detection, escalation and response of incidents.</p> <p>PI - 3. Azure DevOps performs input validation to restrict any non-permissible requests to the API.</p> <p>SOC2 - 12. The security baselines are refreshed for Azure DevOps on a periodic basis.</p> <p>CM - 1. Procedures for managing different types of changes to the features are documented and communicated.</p> <p>C5 - 11. Azure DevOps has implemented tools to perform integrity verification checks to detect unauthorized changes to software, firmware and information.</p>	

SYSTEM OPERATIONS

Trust Criteria	Azure DevOps Activity	Test Result
<p>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.</p>	<p>PI - 3. Azure DevOps performs input validation to restrict any non-permissible requests to the API.</p> <p>SOC2 - 12. The security baselines are refreshed for Azure DevOps on a periodic basis.</p> <p>VM - 1. Production and supporting infrastructure are configured to log and collect security events.</p> <p>VM - 2. Administrator activity is logged.</p> <p>VM - 3. A monitoring system is implemented on production and supporting infrastructure to monitor the service for potential malicious activity and intrusion past service trust boundaries.</p> <p>VM - 4. Procedures have been established to investigate and respond to the malicious events detected by the monitoring system for timely resolution.</p> <p>VM - 5. Procedures are established to evaluate and implement Microsoft released patches to service components.</p> <p>VM - 6. Procedures are established to monitor production and supporting infrastructure for known security vulnerabilities. Identified security vulnerabilities are remediated.</p> <p>CM - 6. Any changes to production via break-glass have been reviewed to ensure all changes were appropriate.</p> <p>C5 - 11. Azure DevOps has implemented tools to perform integrity verification checks to detect unauthorized changes to software, firmware and information.</p>	<p>No exceptions noted.</p>
<p>CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and</p>	<p>VM - 1. Production and supporting infrastructure are configured to log and collect security events.</p> <p>VM - 2. Administrator activity is logged.</p>	<p>No exceptions noted.</p>

Trust Criteria	Azure DevOps Activity	Test Result
errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	<p>VM - 3. A monitoring system is implemented on production and supporting infrastructure to monitor the service for potential malicious activity and intrusion past service trust boundaries.</p> <p>VM - 4. Procedures have been established to investigate and respond to the malicious events detected by the monitoring system for timely resolution.</p> <p>VM - 5. Procedures are established to evaluate and implement Microsoft released patches to service components.</p> <p>VM - 6. Procedures are established to monitor production and supporting infrastructure for known security vulnerabilities. Identified security vulnerabilities are remediated.</p> <p>VM - 7. The availability of the service is monitored through third-party and internal tools, and the status is communicated through a Service Dashboard.</p> <p>VM - 9. Azure DevOps provides logging mechanisms that can be configured by customers to log activities and metrics.</p> <p>IM - 1. An incident management framework is established and communicated with defined processes, roles and responsibilities for the detection, escalation and response of incidents.</p> <p>IM - 3. The Service Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures.</p> <p>DS - 5. Backups of key service components are performed regularly and stored in fault tolerant (isolated) facilities. Backups are monitored and backup errors are investigated and followed-up on appropriately.</p> <p>DS - 6. Critical Azure DevOps components are designed with redundancy to sustain isolated faults and minimize disruptions to customer services.</p>	

Trust Criteria	Azure DevOps Activity	Test Result
	<p>SOC2 - 12. The security baselines are refreshed for Azure DevOps on a periodic basis.</p> <p>C5 - 11. Azure DevOps has implemented tools to perform integrity verification checks to detect unauthorized changes to software, firmware and information.</p>	
<p>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.</p>	<p>IM - 1. An incident management framework is established and communicated with defined processes, roles and responsibilities for the detection, escalation and response of incidents.</p> <p>IM - 2. Events, thresholds and metrics are defined and configured to detect incidents and alert the associated Service Operations team.</p> <p>IM - 3. The Service Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures.</p> <p>IM - 4. Incident post-mortem activities are conducted for high severity incidents impacting the service environment.</p> <p>VM - 4. Procedures have been established to investigate and respond to the malicious events detected by the monitoring system for timely resolution.</p> <p>SOC2 - 3. The service maintains a customer support website that describes the process for customers and other external users to inform about potential security issues and submitting complaints. Reported issues are reviewed and addressed per documented incident management procedures.</p>	No exceptions noted.
<p>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.</p>	<p>IM - 1. An incident management framework is established and communicated with defined processes, roles and responsibilities for the detection, escalation and response of incidents.</p>	No exceptions noted.

Trust Criteria	Azure DevOps Activity	Test Result
	<p>IM - 2. Events, thresholds and metrics are defined and configured to detect incidents and alert the associated Service Operations team.</p> <p>IM - 3. The Service Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures.</p> <p>IM - 4. Incident post-mortem activities are conducted for high severity incidents impacting the service environment.</p> <p>VM - 4. Procedures have been established to investigate and respond to the malicious events detected by the monitoring system for timely resolution.</p> <p>VM - 7. The availability of the service is monitored through third-party and internal tools, and the status is communicated through a Service Dashboard.</p> <p>SOC2 - 3. The service maintains a customer support website that describes the process for customers and other external users to inform about potential security issues and submitting complaints. Reported issues are reviewed and addressed per documented incident management procedures.</p> <p>SOC2 - 6. The service maintains and notifies customers of potential changes, and security and availability type of events that may impact the service, through an online Service Dashboard. Changes to the security commitments and security obligations of the service's customers are updated on the Azure DevOps website in a timely manner.</p>	
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.	IM - 1. An incident management framework is established and communicated with defined processes, roles and responsibilities for the detection, escalation and response of incidents.	No exceptions noted.

Trust Criteria	Azure DevOps Activity	Test Result
	<p>IM - 2. Events, thresholds and metrics are defined and configured to detect incidents and alert the associated Service Operations team.</p> <p>IM - 3. The Service Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures.</p> <p>IM - 4. Incident post-mortem activities are conducted for high severity incidents impacting the service environment.</p> <p>VM - 4. Procedures have been established to investigate and respond to the malicious events detected by the monitoring system for timely resolution.</p> <p>VM - 5. Procedures are established to evaluate and implement Microsoft released patches to service components.</p> <p>SOC2 - 3. The service maintains a customer support website that describes the process for customers and other external users to inform about potential security issues and submitting complaints. Reported issues are reviewed and addressed per documented incident management procedures.</p> <p>BC - 4. The BCP team conducts testing of the business continuity and disaster recovery plans at least annually. Issues identified during testing are resolved during the exercises and plans are updated accordingly.</p>	

CHANGE MANAGEMENT

Trust Criteria	Azure DevOps Activity	Test Result
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.	<p>SDL - 1. Development of new features and changes to existing features follow a defined approach based on the Microsoft Secure Development Lifecycle (SDL) methodology.</p> <p>SDL - 2. Applicable operational security and internal control requirements are documented and approved for Azure DevOps.</p> <p>SDL - 3. Responsibilities for production deployment are segregated within the feature teams.</p> <p>SDL - 4. Separate environments, outside of production, are established for the purpose of developing and testing changes. Production data is not replicated in test or development environments.</p> <p>SDL - 5. Azure DevOps services use code repositories for managing source code changes. Procedures are established to authorize access for personnel based on their role and submit changes to source code. Code changes submitted to the code repository are logged and can be traced to the individuals or system components executing them.</p> <p>SDL - 6. A security review of releases is performed on a periodic basis by designated security personnel within Azure DevOps.</p> <p>SDL - 7. Source code builds are scanned for malware prior to release to production.</p> <p>DS - 4. Cryptographic controls are used for information protection within the platform based on the Cryptographic Policy and Key Management procedures.</p> <p>VM - 5. Procedures are established to evaluate and implement Microsoft released patches to service components.</p> <p>IM - 4. Incident post-mortem activities are conducted for high severity incidents impacting the service environment.</p>	No exceptions noted.

Trust Criteria	Azure DevOps Activity	Test Result
	<p>SOC2 - 1. Service assets are classified in accordance with Microsoft Online Services Classification Guidelines. Microsoft has conducted security categorization for its information and information systems and the results are documented, reviewed and approved by the authorizing official.</p> <p>SOC2 - 2. The service maintains an inventory of key information assets. Procedures are established to review usage of key information assets on at least an annual basis.</p> <p>SOC2 - 12. The security baselines are refreshed for Azure DevOps on a periodic basis.</p> <p>SOC2 - 15. Microsoft performs annual Information Security Management System (ISMS) review and results are reviewed with management.</p> <p>This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.</p> <p>CM - 1. Procedures for managing different types of changes to the features are documented and communicated.</p> <p>CM - 2. Key stakeholders approve changes prior to release into production based on documented change management procedures.</p> <p>CM - 3. Responsibilities for approving and implementing changes to the features are segregated among designated personnel.</p> <p>CM - 4. Software releases and configuration changes are tested based on established criteria prior to production implementation.</p> <p>CM - 5. Implemented changes are reviewed for adherence to established procedures prior to closure. Changes are rolled back to their previous state in case of errors or security concerns.</p> <p>CM - 6. Any changes to production via break-glass have been reviewed to ensure all changes were appropriate.</p>	

Trust Criteria	Azure DevOps Activity	Test Result
	C5 - 11. Azure DevOps has implemented tools to perform integrity verification checks to detect unauthorized changes to software, firmware and information.	

RISK MITIGATION

Trust Criteria	Azure DevOps Activity	Test Result
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	<p>SOC2 - 15. Microsoft performs annual Information Security Management System (ISMS) review and results are reviewed with management.</p> <p>This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.</p> <p>BC - 1. Management conducts a risk assessment to identify and assess continuity risks related to Azure DevOps. The Business Impact Analysis is carried out and impacts are assessed for critical services based on revenue and operations considerations.</p>	No exceptions noted.
CC9.2 The entity assesses and manages risks associated with vendors and business partners.	SOC2 - 17. Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within Azure DevOps environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Legal and Corporate Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements.	No exceptions noted.

Trust Criteria	Azure DevOps Activity	Test Result
	<p>IS - 4. An information security education and awareness program is established that includes policy training and periodic security updates to Azure DevOps personnel.</p> <p>ELC - 5. Internal Audit Charter directs Internal Audit to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment.</p> <p>ELC - 6. Management expects outsourced providers to meet certain levels of skills and experience, depending on the role and holds them accountable to achieving specific deliverables, as outlined in a Statement of Work. Outsourced providers are trained to understand and comply with Microsoft's supplier code of conduct.</p> <p>ELC - 9. The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management.</p> <p>C5 - 9. Prior to contracting with Microsoft, suppliers undergo a risk assessment based on the services that will be provided and data handled. List of reviewed suppliers is maintained and their risk profiles are reviewed at least annually.</p>	

ADDITIONAL CRITERIA FOR AVAILABILITY

Trust Criteria	Azure DevOps Activity	Test Result
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.	<p>BC - 3. Microsoft has developed a Business Continuity and Disaster Recovery (BC / DR) Standard Operating Procedure and documentation that includes the defined information security and availability requirements.</p> <p>BC - 5. Management has established monitoring mechanisms to address capacity issues in a timely manner.</p> <p>PI - 2. Azure DevOps management reviews portal performance periodically to evaluate compliance with customer SLA requirements.</p> <p>VM - 7. The availability of the service is monitored through third-party and internal tools, and the status is communicated through a Service Dashboard.</p>	No exceptions noted.
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.	<p>DS - 5. Backups of key service components are performed regularly and stored in fault tolerant (isolated) facilities. Backups are monitored and backup errors are investigated and followed-up on appropriately.</p> <p>DS - 6. Critical Azure DevOps components are designed with redundancy to sustain isolated faults and minimize disruptions to customer services.</p> <p>DS - 7. Customer data is automatically replicated to minimize isolated faults. Customers are able to determine geographical regions of the data processing and storage, including data backups.</p> <p>DS - 8. Upon termination of a customer account, the customer data is removed based upon the stipulated retention and removal timelines.</p> <p>BC - 2. Business Continuity Plans (BCP) are documented and published for critical services, which provide roles and responsibilities and detailed procedures for recovery and reconstitution of systems to a known state per defined Recovery</p>	No exceptions noted.

Trust Criteria	Azure DevOps Activity	Test Result
	<p>Time Objectives (RTO) and Recovery Point Objectives (RPO). Plans are reviewed on an annual basis, at a minimum.</p> <p>BC - 3. Microsoft has developed a Business Continuity and Disaster Recovery (BC / DR) Standard Operating Procedure and documentation that includes the defined information security and availability requirements.</p>	
A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.	<p>BC - 2. Business Continuity Plans (BCP) are documented and published for critical services, which provide roles and responsibilities and detailed procedures for recovery and reconstitution of systems to a known state per defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Plans are reviewed on an annual basis, at a minimum.</p> <p>BC - 4. The BCP team conducts testing of the business continuity and disaster recovery plans at least annually. Issues identified during testing are resolved during the exercises and plans are updated accordingly.</p>	No exceptions noted.

ADDITIONAL CRITERIA FOR CONFIDENTIALITY

Trust Criteria	Azure DevOps Activity	Test Result
<p>C1.1 The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.</p>	<p>DS - 7. Customer data is automatically replicated to minimize isolated faults. Customers are able to determine geographical regions of the data processing and storage, including data backups.</p> <p>DS - 8. Upon termination of a customer account, the customer data is removed based upon the stipulated retention and removal timelines.</p> <p>OA - 3. Procedures are in place to disable accounts on a timely basis, upon the user's termination.</p> <p>SOC2 - 1. Service assets are classified in accordance with Microsoft Online Services Classification Guidelines. Microsoft has conducted security categorization for its information and information systems and the results are documented, reviewed and approved by the authorizing official.</p> <p>SOC2 - 10. Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees must acknowledge Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage.</p>	<p>No exceptions noted.</p>
<p>C1.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality.</p>	<p>SOC2 - 10. Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees must acknowledge Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage.</p> <p>DS - 8. Upon termination of a customer account, the customer data is removed based upon the stipulated retention and removal timelines.</p>	<p>No exceptions noted.</p>

Trust Criteria	Azure DevOps Activity	Test Result
	C5 - 4. Customer metadata is collected, retained, and removed based on the documented procedures.	

ADDITIONAL CRITERIA FOR PROCESSING INTEGRITY

Trust Criteria	Azure DevOps Activity	Test Result
PI1.1 The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.	<p>DS - 8. Upon termination of a customer account, the customer data is removed based upon the stipulated retention and removal timelines.</p> <p>PI - 3. Azure DevOps performs input validation to restrict any non-permissible requests to the API.</p> <p>SOC2 - 4. The service maintains and communicates the confidentiality and related security obligations for customer data via the Microsoft Trust Center. Guidelines and recommendations for the secure use of the cloud services, as applicable, are communicated to customers.</p> <p>SOC2 - 5. The service maintains and distributes an accurate system description to authorized users.</p> <p>SOC2 - 7. Prior to engaging in service, customers are required to review and agree with the acceptable use of data and the Service, as well as security and privacy requirements, which are defined in the Microsoft Online Services Use Rights, Microsoft Online Subscription Agreement, Privacy Statement and Technical Overview of the Security Features.</p> <p>C5 - 13. Customer data is accessible within agreed upon services in data formats compatible with providing those services.</p>	No exceptions noted.

Trust Criteria	Azure DevOps Activity	Test Result
PI1.2 The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.	<p>PI - 3. Azure DevOps performs input validation to restrict any non-permissible requests to the API.</p> <p>PI - 4. Azure DevOps appropriately provisions the services based on request from customer through the portal/API.</p>	No exceptions noted.
PI1.3 The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.	<p>IM - 3. The Service Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures.</p> <p>PI - 1. Azure DevOps monitors the transactions invoked by the customer and relays them appropriately to the designated endpoint. Actions are taken in response to defined threshold events.</p> <p>PI - 2. Azure DevOps management reviews portal performance periodically to evaluate compliance with customer SLA requirements.</p> <p>PI - 4. Azure DevOps appropriately provisions the services based on request from customer through the portal/API.</p> <p>CM - 1. Procedures for managing different types of changes to the features are documented and communicated.</p> <p>CM - 4. Software releases and configuration changes are tested based on established criteria prior to production implementation.</p> <p>CM - 5. Implemented changes are reviewed for adherence to established procedures prior to closure. Changes are rolled back to their previous state in case of errors or security concerns.</p> <p>OA - 1. Administrative access to the service is controlled through defined interfaces that require authentication using AD credentials.</p> <p>OA - 2. Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning access to employees, contractors, and service providers to specific applications or information resources.</p>	No exceptions noted.

Trust Criteria	Azure DevOps Activity	Test Result
	<p>OA - 3. Procedures are in place to disable accounts on a timely basis, upon the user's termination.</p> <p>OA - 5. Access privileges are reviewed quarterly to determine if access rights are commensurate to the user's job duties. Access is modified based on the results of the reviews.</p> <p>OA - 6. Procedures are established for granting temporary access for personnel to customer data and applications upon appropriate approval.</p> <p>OA - 8. Alerts are generated when a break-glass account is used to access production environment.</p> <p>OA - 10. Access to production resources requires the use of a Secure Admin Workstation (SAW) which requires MFA for access. SAWs are hardened and secured devices with restricted access.</p> <p>DS - 5. Backups of key service components are performed regularly and stored in fault tolerant (isolated) facilities. Backups are monitored and backup errors are investigated and followed-up on appropriately.</p> <p>DS - 6. Critical Azure DevOps components are designed with redundancy to sustain isolated faults and minimize disruptions to customer services.</p> <p>DS - 7. Customer data is automatically replicated to minimize isolated faults. Customers are able to determine geographical regions of the data processing and storage, including data backups.</p>	
PI1.4 The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.	<p>CM - 1. Procedures for managing different types of changes to the features are documented and communicated.</p> <p>CM - 4. Software releases and configuration changes are tested based on established criteria prior to production implementation.</p>	No exceptions noted.

Trust Criteria	Azure DevOps Activity	Test Result
	<p>DS - 8. Upon termination of a customer account, the customer data is removed based upon the stipulated retention and removal timelines.</p> <p>IM - 3. The Service Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures.</p> <p>PI - 4. Azure DevOps appropriately provisions the services based on request from customer through the portal/API.</p> <p>LA - 3. Logical segregation is implemented to restrict unauthorized access to other customer tenants.</p> <p>C5 - 11. Azure DevOps has implemented tools to perform integrity verification checks to detect unauthorized changes to software, firmware and information.</p>	
<p>PI1.5 The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.</p>	<p>DS - 5. Backups of key service components are performed regularly and stored in fault tolerant (isolated) facilities. Backups are monitored and backup errors are investigated and followed-up on appropriately.</p> <p>DS - 6. Critical Azure DevOps components are designed with redundancy to sustain isolated faults and minimize disruptions to customer services.</p> <p>DS - 8. Upon termination of a customer account, the customer data is removed based upon the stipulated retention and removal timelines.</p> <p>OA - 1. Administrative access to the service is controlled through defined interfaces that require authentication using AD credentials.</p>	<p>No exceptions noted.</p>

Part B: C5 Criteria, Control Activities provided by Microsoft, and Test Results provided by Deloitte & Touche LLP

OIS: Organization of Information Security

Control Objective 5.1: Plan, implement, maintain and continuously improve the information security framework within the organisation.

C5 Criteria	Azure DevOps Activity	Test Result
<p>OIS-01 The Cloud Service Provider operates an information security management system (ISMS) in accordance with ISO/IEC 27001. The scope of the ISMS covers the Cloud Service Provider's organisational units, locations and procedures for providing the cloud service.</p> <p>The measures for setting up, implementing, maintaining and continuously improving the ISMS are documented.</p> <p>The documentation includes:</p> <ul style="list-style-type: none"> • Scope of the ISMS (Section 4.3 of ISO/IEC 27001); • Declaration of applicability (Section 6.1.3), and • Results of the last management review (Section 9.3). 	<p>SOC2 - 15. Microsoft performs annual Information Security Management System (ISMS) review and results are reviewed with management.</p> <p>This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.</p> <p>C5 - 1. Standard Operating Procedures (SOPs), that define the procedures required to operate and maintain the Service environment, have been established and communicated to employees. SOPs are reviewed and approved annually by appropriate management.</p>	<p>No exceptions noted.</p>
<p>OIS-02 The top management of the Cloud Service Provider has adopted an information security policy and communicated it to internal and external employees as well as cloud customers.</p> <p>The policy describes:</p>	<p>IS - 1. Microsoft has documented and communicated a security policy that defines the information security rules and requirements for the Azure DevOps environment.</p> <p>IS - 2. The security policy is reviewed and approved annually by Microsoft management.</p> <p>IS - 3. Management has established defined roles and responsibilities to oversee implementation of the information security policy across the service.</p>	<p>No exceptions noted.</p>

C5 Criteria	Azure DevOps Activity	Test Result
<ul style="list-style-type: none"> the importance of information security, based on the requirements of cloud customers in relation to information security; the security objectives and the desired security level, based on the business goals and tasks of the Cloud Service Provider; the most important aspects of the security strategy to achieve the security objectives set; and the organisational structure for information security in the ISMS application area. 	<p>IS - 4. An information security education and awareness program is established that includes policy training and periodic security updates to Azure DevOps personnel.</p>	
<p>OIS-03 Interfaces and dependencies between cloud service delivery activities performed by the Cloud Service Provider and activities performed by third parties are documented and communicated. This includes dealing with the following events:</p> <ul style="list-style-type: none"> Vulnerabilities; Security incidents; and Malfunctions. <p>The type and scope of the documentation is geared towards the information requirements of the subject matter experts of the affected organisations in order to carry out the activities appropriately (e.g. definition of roles and responsibilities in guidelines, description of cooperation obligations in service descriptions and contracts).</p> <p>The communication of changes to the interfaces and dependencies takes place in a</p>	<p>IS - 3. Management has established defined roles and responsibilities to oversee implementation of the information security policy across the service.</p> <p>IM - 1. An incident management framework is established and communicated with defined processes, roles and responsibilities for the detection, escalation and response of incidents.</p> <p>SOC2 - 3. The service maintains a customer support website that describes the process for customers and other external users to inform about potential security issues and submitting complaints. Reported issues are reviewed and addressed per documented incident management procedures.</p> <p>SOC2 - 4. The service maintains and communicates the confidentiality and related security obligations for customer data via the Microsoft Trust Center. Guidelines and recommendations for the secure use of the cloud services, as applicable, are communicated to customers.</p> <p>SOC2 - 6. The service maintains and notifies customers of potential changes, and security and availability type of events that may impact the service, through an online Service Dashboard. Changes to the security commitments and security obligations of the service's customers are updated on the Azure DevOps website in a timely manner.</p>	<p>No exceptions noted.</p>

C5 Criteria	Azure DevOps Activity	Test Result
timely manner so that the affected organisations and third parties can react appropriately with organisational and technical measures before the changes take effect.	SOC2 - 10. Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees must acknowledge Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage.	
<p>OIS-04 Conflicting tasks and responsibilities are separated based on an OIS-06 risk assessment to reduce the risk of unauthorised or unintended changes or misuse of cloud customer data processed, stored or transmitted in the cloud service.</p> <p>The risk assessment covers the following areas, insofar as these are applicable to the provision of the Cloud Service and are in the area of responsibility of the Cloud Service Provider:</p> <ul style="list-style-type: none"> • Administration of rights profiles, approval and assignment of access and access authorisations (cf. IDM-01); • Development, testing and release of changes (cf. DEV-01); and • Operation of the system components. <p>If separation cannot be established for organisational or technical reasons, measures are in place to monitor the activities in order to detect unauthorised or unintended changes as well as misuse and to take appropriate actions.</p>	<p>SOC2 - 13. Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization.</p> <p>SOC2 - 18. Microsoft Azure DevOps performs an annual risk assessment that covers security, continuity, and operational risks. As part of this process, threats to security are identified and risks from these threats are formally assessed.</p> <p>C5 - 11. Azure DevOps has implemented tools to perform integrity verification checks to detect unauthorized changes to software, firmware and information.</p> <p>OA - 8. Alerts are generated when a break-glass account is used to access production environment.</p> <p>CM - 3. Responsibilities for approving and implementing changes to the features are segregated among designated personnel.</p> <p>CM - 6. Any changes to production via break-glass have been reviewed to ensure all changes were appropriate.</p> <p>SDL - 3. Responsibilities for production deployment are segregated within the feature teams.</p> <p>PI - 4. Azure DevOps appropriately provisions the services based on request from customer through the portal/API.</p>	No exceptions noted.
OIS-05 The Cloud Service Provider leverages relevant authorities and interest	SOC2 - 13. Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined,	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
groups in order to stay informed about current threats and vulnerabilities. The information flows into the procedures for handling risks (cf. OIS-06) and vulnerabilities (cf. OPS-19).	documented, and kept up to date for each information system and the organization. SOC2 - 14. Microsoft manages a compliance program with representation from various cross-functional teams including CELA, Marketing, security champions to identify and manage compliance with relevant statutory, regulatory and contractual requirements.	
<p>OIS-06 Policies and instructions for risk management procedures are documented, communicated and provided in accordance with SP-01 for the following aspects:</p> <ul style="list-style-type: none"> • Identification of risks associated with the loss of confidentiality, integrity, availability and authenticity of information within the scope of the ISMS and assigning risk owners; • Analysis of the probability and impact of occurrence and determination of the level of risk; • Evaluation of the risk analysis based on defined criteria for risk acceptance and prioritisation of handling; • Handling of risks through measures, including approval of authorisation and acceptance of residual risks by risk owners; and • Documentation of the activities implemented to enable consistent, valid and comparable results. 	<p>SOC2 - 17. Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within Azure DevOps environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Legal and Corporate Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements.</p> <p>SOC2 - 18. Microsoft Azure DevOps performs an annual risk assessment that covers security, continuity, and operational risks. As part of this process, threats to security are identified and risks from these threats are formally assessed.</p> <p>ELC - 9. The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management.</p>	No exceptions noted.
OIS-07 The Cloud Service Provider executes the process for handling risks as needed or	SOC2 - 17. Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within Azure DevOps	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
<p>at least once a year. The following aspects are taken into account when identifying risks, insofar as they are applicable to the cloud service provided and are within the area of responsibility of the Cloud Service Provider:</p> <ul style="list-style-type: none"> • Processing, storage or transmission of data of cloud customers with different protection needs; • Occurrence of vulnerabilities and malfunctions in technical protective measures for separating shared resources; • Attacks via access points, including interfaces accessible from public networks; • Conflicting tasks and areas of responsibility that cannot be separated for organisational or technical reasons; and • Dependencies on subservice organisations. <p>The analysis, evaluation and treatment of risks, including the approval of actions and acceptance of residual risks, is reviewed for adequacy at least annually by the risk owners.</p>	<p>environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Legal and Corporate Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements.</p> <p>SOC2 - 18. Microsoft Azure DevOps performs an annual risk assessment that covers security, continuity, and operational risks. As part of this process, threats to security are identified and risks from these threats are formally assessed.</p> <p>ELC - 9. The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management.</p>	

SP: Security Policies and Instructions

Control Objective 5.2: Provide policies and instructions regarding security requirements and to support business requirements.

C5 Criteria	Azure DevOps Activity	Test Result
<p>SP-01. Policies and instructions (incl. concepts and guidelines) are derived from the information security policy and are documented according to a uniform structure. They are communicated and made available to all internal and external employees of the Cloud Service Provider in an appropriate manner</p> <p>The policies and instructions are version controlled and approved by the top management of the Cloud Service Provider or an authorised body</p> <p>The policies and instructions describe at least the following aspects:</p> <ul style="list-style-type: none">• Objectives;• Scope;• Roles and responsibilities, including staff qualification requirements and the establishment of substitution rules;• Roles and dependencies on other organisations (especially cloud customers and subservice organisations);• Steps for the execution of the security strategy; and• Applicable legal and regulatory requirements.	<p>C5 - 1. Standard Operating Procedures (SOPs), that define the procedures required to operate and maintain the Service environment, have been established and communicated to employees. SOPs are reviewed and approved annually by appropriate management.</p> <p>IS - 1. Microsoft has documented and communicated a security policy that defines the information security rules and requirements for the Azure DevOps environment.</p> <p>IS - 2. The security policy is reviewed and approved annually by Microsoft management.</p> <p>IS - 3. Management has established defined roles and responsibilities to oversee implementation of the information security policy across the service.</p> <p>IS - 4. An information security education and awareness program is established that includes policy training and periodic security updates to Azure DevOps personnel.</p> <p>SOC2 - 13. Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization.</p> <p>SOC2 - 14. Microsoft manages a compliance program with representation from various cross-functional teams including CELA, Marketing, security champions to identify and manage compliance with relevant statutory, regulatory and contractual requirements.</p>	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
<p>SP-02. Information security policies and instructions are reviewed at least annually for adequacy by the Cloud Service Provider's subject matter experts.</p> <p>The review shall consider at least the following aspects:</p> <ul style="list-style-type: none"> • Organisational and technical changes in the procedures for providing the cloud service; and • Legal and regulatory changes in the Cloud Service Provider's environment. <p>Revised policies and instructions are approved before they become effective.</p>	<p>C5 - 1. Standard Operating Procedures (SOPs), that define the procedures required to operate and maintain the Service environment, have been established and communicated to employees. SOPs are reviewed and approved annually by appropriate management.</p> <p>IS - 2. The security policy is reviewed and approved annually by Microsoft management.</p> <p>SOC2 - 13. Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization.</p> <p>SOC2 - 14. Microsoft manages a compliance program with representation from various cross-functional teams including CELA, Marketing, security champions to identify and manage compliance with relevant statutory, regulatory and contractual requirements.</p> <p>SOC2 - 15. Microsoft performs annual Information Security Management System (ISMS) review and results are reviewed with management.</p> <p>This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.</p>	<p>No exceptions noted.</p>
<p>SP-03 Exceptions to the policies and instructions for information security as well as respective controls go through the OIS-06 risk management process, including approval of these exceptions and acceptance of the associated risks by the risk owners. The approvals of exceptions are documented, limited in time and are reviewed for appropriateness at least annually by the risk owners.</p>	<p>SOC2 - 17. Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within Azure DevOps environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Legal and Corporate Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements.</p> <p>SOC2 - 18. Microsoft Azure DevOps performs an annual risk assessment that covers security, continuity, and operational risks. As part of this process, threats to security are identified and risks from these threats are formally assessed.</p> <p>C5 - 12. Management has developed and documented a risk assessment policy to address the purpose, scope, roles, responsibilities for managing deviations from</p>	<p>No exceptions noted.</p>

C5 Criteria	Azure DevOps Activity	Test Result
	the security policies/standards. The risk assessment policy and procedures are reviewed and updated on an annual basis.	

HR: Personnel

Control Objective 5.3: Ensure that employees understand their responsibilities, are aware of their responsibilities with regard to information security, and that the organisation's assets are protected in the event of changes in responsibilities or termination.

C5 Criteria	Azure DevOps Activity	Test Result
<p>HR-01 The competency and integrity of all internal and external employees of the Cloud Service Provider with access to cloud customer data or system components under the Cloud Service Provider's responsibility who are responsible to provide the cloud service in the production environment shall be verified prior to commencement of employment in accordance with local legislation and regulation by the Cloud Service Provider.</p> <p>To the extent permitted by law, the review will cover the following areas:</p> <ul style="list-style-type: none"> • Verification of the person through identity card; • Verification of the CV; • Verification of academic titles and degrees; 	<p>SOC2 - 9. Microsoft personnel and contingent staff undergo formal screening, including background verification checks as a part of the hiring process prior to being granted access. Additional screening is conducted in accordance with customer specific requirements, for employees with access to applicable data.</p> <p>ELC - 7. Employees hold periodic connects with their managers to validate they are on the expected career path and facilitate greater collaboration. Employees also review their performance against their documented deliverables (priorities) and discuss the results with their managers.</p>	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
<ul style="list-style-type: none"> • Request of a police clearance certificate for applicants; • Certificate of good conduct or national equivalent; and • Evaluation of the risk to be blackmailed. 		
<p>HR-02 The Cloud Service Provider's internal and external employees are required by the employment terms and conditions to comply with applicable policies and instructions relating to information security.</p> <p>The information security policy, and the policies and instructions based on it, are to be acknowledged by the internal and external personnel in a documented form before access is granted to any cloud customer data or system components under the responsibility of the Cloud Service Provider used to provide the cloud service in the production environment.</p>	<p>SOC2 - 10. Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees must acknowledge Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage.</p> <p>ELC - 2. Microsoft Compliance and Ethics team updates the Standards of Business Conduct (SBC) as necessary and the Code is made available internally and externally. The SBC reflects Microsoft's continued commitment to ethical business practices and regulatory compliance. Compliance and Ethics team provides an annual Standards of Business Conduct training course that is mandatory for all employees. Employees who do not complete the training on time are tracked and followed up with appropriately.</p> <p>IS - 4. An information security education and awareness program is established that includes policy training and periodic security updates to Azure DevOps personnel.</p>	No exceptions noted.
<p>HR-03 The Cloud Service Provider operates a target group-oriented security awareness and training program, which is completed by all internal and external employees of the Cloud Service Provider on a regular basis. The program is regularly updated based on changes to policies and instructions and the current threat situation and includes the following aspects:</p>	<p>IS - 4. An information security education and awareness program is established that includes policy training and periodic security updates to Azure DevOps personnel.</p> <p>ELC - 6. Management expects outsourced providers to meet certain levels of skills and experience, depending on the role and holds them accountable to achieving specific deliverables, as outlined in a Statement of Work. Outsourced providers are trained to understand and comply with Microsoft's supplier code of conduct.</p>	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
<ul style="list-style-type: none"> • Handling system components used to provide the cloud service in the production environment in accordance with applicable policies and procedures; • Handling cloud customer data in accordance with applicable policies and instructions and applicable legal and regulatory requirements; • Information about the current threat situation; and • Correct behaviour in the event of security incidents. 		
<p>HR-04 In the event of violations of policies and instructions or applicable legal and regulatory requirements, actions are taken in accordance with a defined policy that includes the following aspects:</p> <ul style="list-style-type: none"> • Verifying whether a violation has occurred; and • Consideration of the nature and severity of the violation and its impact. <p>The internal and external employees of the Cloud Service Provider are informed about possible disciplinary measures.</p> <p>The use of disciplinary measures is appropriately documented.</p>	<p>SOC2 - 8. Microsoft has defined disciplinary actions for employees and contingent staff that commit a security breach or violate the security policy.</p>	<p>No exceptions noted.</p>
<p>HR-05 Internal and external employees have been informed about which</p>	<p>SOC2 - 10. Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon</p>	<p>No exceptions noted.</p>

C5 Criteria	Azure DevOps Activity	Test Result
responsibilities, arising from employment terms and conditions relating to information security, will remain in place when their employment is terminated or changed and for how long.	<p>hire. In addition, employees must acknowledge Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage.</p> <p>ELC - 2. Microsoft Compliance and Ethics team updates the Standards of Business Conduct (SBC) as necessary and the Code is made available internally and externally. The SBC reflects Microsoft's continued commitment to ethical business practices and regulatory compliance. Compliance and Ethics team provides an annual Standards of Business Conduct training course that is mandatory for all employees. Employees who do not complete the training on time are tracked and followed up with appropriately.</p>	
<p>HR-06 The non-disclosure or confidentiality agreements to be agreed with internal employees, external service providers and suppliers of the Cloud Service Provider are based on the requirements identified by the Cloud Service Provider for the protection of confidential information and operational details.</p> <p>The agreements are to be accepted by external service providers and suppliers when the contract is agreed. The agreements must be accepted by internal employees of the Cloud Service Provider before authorisation to access data of cloud customers is granted.</p> <p>The requirements must be documented and reviewed at regular intervals (at least annually). If the review shows that the requirements need to be adapted, the non-disclosure or confidentiality agreements are updated.</p>	<p>SOC2 - 4. The service maintains and communicates the confidentiality and related security obligations for customer data via the Microsoft Trust Center. Guidelines and recommendations for the secure use of the cloud services, as applicable, are communicated to customers.</p> <p>SOC2 - 6. The service maintains and notifies customers of potential changes, and security and availability type of events that may impact the service, through an online Service Dashboard. Changes to the security commitments and security obligations of the service's customers are updated on the Azure DevOps website in a timely manner.</p> <p>SOC2 - 10. Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees must acknowledge Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage.</p> <p>SOC2 - 17. Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within Azure DevOps environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Legal and Corporate Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements.</p>	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
The Cloud Service Provider must inform the internal employees, external service providers and suppliers and obtain confirmation of the updated confidentiality or non-disclosure agreement.		

AM: Asset Management

Control Objective 5.4: Identify the organisation's own assets and ensure an appropriate level of protection throughout their lifecycle.

C5 Criteria	Azure DevOps Activity	Test Result
<p>AM-01 The Cloud Service Provider has established procedures for inventorying assets.</p> <p>The inventory is performed automatically and/or by the people or teams responsible for the assets to ensure complete, accurate, valid and consistent inventory throughout the asset lifecycle.</p> <p>Assets are recorded with the information needed to apply the Risk Management Procedure (Cf. OIS-07), including the measures taken to manage these risks throughout the asset lifecycle. Changes to this information are logged.</p>	<p>SOC2 - 1. Service assets are classified in accordance with Microsoft Online Services Classification Guidelines. Microsoft has conducted security categorization for its information and information systems and the results are documented, reviewed and approved by the authorizing official.</p> <p>SOC2 - 2. The service maintains an inventory of key information assets. Procedures are established to review usage of key information assets on at least an annual basis.</p>	No exceptions noted.
<p>AM-02 Policies and instructions for acceptable use and safe handling of assets are documented, communicated and</p>	<p>SOC2 - 1. Service assets are classified in accordance with Microsoft Online Services Classification Guidelines. Microsoft has conducted security categorization</p>	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
<p>provided in accordance with SP-01 and address the following aspects of the asset lifecycle as applicable to the asset:</p> <ul style="list-style-type: none"> • Approval procedures for acquisition, commissioning, maintenance, decommissioning, and disposal by authorised personnel or system components; • Inventory; • Classification and labelling based on the need for protection of the information and measures for the level of protection identified; • Secure configuration of mechanisms for error handling, logging, encryption, authentication and authorisation; • Requirements for versions of software and images as well as application of patches; • Handling of software for which support and security patches are not available anymore; • Restriction of software installations or use of services; • Protection against malware; • Remote deactivation, deletion or blocking; • Physical delivery and transport; • dealing with incidents and vulnerabilities; and • Complete and irrevocable deletion of the data upon decommissioning. 	<p>for its information and information systems and the results are documented, reviewed and approved by the authorizing official.</p> <p>SOC2 - 10. Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees must acknowledge Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage.</p> <p>C5 - 10. Microsoft has established policies for mobile computing devices to meet appropriate security practices prior to being connected to the production environment.</p>	

C5 Criteria	Azure DevOps Activity	Test Result
<p>AM-03 The Cloud Service Provider has an approval process for the use of hardware to be commissioned, which is used to provide the cloud service in the production environment, in which the risks arising from the commissioning are identified, analysed and mitigated. Approval is granted after verification of the secure configuration of the mechanisms for error handling, logging, encryption, authentication and authorisation according to the intended use and based on the applicable policies.</p>	<p>This C5 criteria is not applicable to Azure DevOps due to the following reasons:</p> <p>Azure is responsible for hardware change management including commissioning and decommissioning.</p>	<p>No exceptions noted.</p>
<p>AM-04 The decommissioning of hardware used to operate system components supporting the cloud service production environment under the responsibility of the Cloud Service Provider requires approval based on the applicable policies.</p> <p>The decommissioning includes the complete and permanent deletion of the data or proper destruction of the media.</p>	<p>This C5 criteria is not applicable to Azure DevOps due to the following reasons:</p> <p>Azure is responsible for hardware change management including commissioning and decommissioning.</p>	<p>No exceptions noted.</p>
<p>AM-05 The Cloud Service Provider's internal and external employees are provably committed to the policies and instructions for acceptable use and safe handling of assets before they can be used if the Cloud Service Provider has determined in a risk assessment that loss or unauthorised access could compromise the information security of the Cloud Service.</p>	<p>SOC2 - 10. Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees must acknowledge Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage.</p> <p>C5 - 10. Microsoft has established policies for mobile computing devices to meet appropriate security practices prior to being connected to the production environment.</p>	<p>No exceptions noted.</p>

C5 Criteria	Azure DevOps Activity	Test Result
Any assets handed over are provably returned upon termination of employment.		
<p>AM-06 Assets are classified and, if possible, labelled. Classification and labelling of an asset reflect the protection needs of the information it processes, stores, or transmits.</p> <p>The need for protection is determined by the individuals or groups responsible for the assets of the Cloud Service Provider according to a uniform schema. The schema provides levels of protection for the confidentiality, integrity, availability, and authenticity protection objectives.</p>	<p>SOC2 - 1. Service assets are classified in accordance with Microsoft Online Services Classification Guidelines. Microsoft has conducted security categorization for its information and information systems and the results are documented, reviewed and approved by the authorizing official.</p> <p>C5 - 10. Microsoft has established policies for mobile computing devices to meet appropriate security practices prior to being connected to the production environment.</p>	No exceptions noted.

PS: Physical Security

Control Objective 5.5: Prevent unauthorised physical access and protect against theft, damage, loss and outage of operations.

C5 Criteria	Azure DevOps Activity	Test Result
<p>PS-01 Security requirements for premises and buildings related to the cloud service provided, are based on the security objectives of the information security policy, identified protection requirements for the cloud service and the assessment of risks to physical and environmental security. The security requirements are documented, communicated and provided in a policy or concept according to SP-01.</p> <p>The security requirements for data centres are based on criteria which comply with established rules of technology. They are suitable for addressing the following risks in accordance with the applicable legal and contractual requirements:</p> <ul style="list-style-type: none">• Faults in planning;• Unauthorised access;• Insufficient surveillance;• Insufficient air-conditioning;• Fire and smoke;• Water;• Power failure; and• Air ventilation and filtration.	<p>This C5 criteria is not applicable to Azure DevOps due to the following reasons:</p> <p>The Physical Security (PS) controls are performed by Microsoft Azure which, as mentioned in the system description, and are carved out within the Azure DevOps SOC 2 report.</p> <p>Azure DevOps does not own, operate or manage PS controls and criteria anticipated by C5.</p>	<p>No exceptions noted.</p>

C5 Criteria	Azure DevOps Activity	Test Result
<p>If the Cloud Service Provider uses premises or buildings operated by third parties to provide the Cloud Service, the document describes which security requirements the Cloud Service Provider places on these third parties.</p> <p>The appropriate and effective verification of implementation is carried out in accordance with the criteria for controlling and monitoring subcontractors (cf. SSO-01, SSO-02).</p>		
<p>PS-02 The cloud service is provided from two locations that are redundant to each other. The locations meet the security requirements of the Cloud Service Provider (cf. PS-01 Security Concept) and are located in an adequate distance to each other to achieve operational redundancy. Operational redundancy is designed in a way that ensures that the availability requirements specified in the service level agreement are met. The functionality of the redundancy is checked at least annually by suitable tests and exercises (cf. BCM-04 - Verification, updating and testing of business continuity).</p>	<p>This C5 criteria is not applicable to Azure DevOps due to the following reasons:</p> <p>The Physical Security (PS) controls are performed by Microsoft Azure which, as mentioned in the system description, and are carved out within the Azure DevOps SOC 2 report.</p> <p>Azure DevOps does not own, operate or manage PS controls and criteria anticipated by C5.</p>	<p>No exceptions noted.</p>
<p>PS-03 The structural shell of premises and buildings related to the cloud service provided are physically solid and protected by adequate security measures that meet the security requirements of the Cloud Service Provider (cf. PS-01 Security Concept).</p>	<p>This C5 criteria is not applicable to Azure DevOps due to the following reasons:</p> <p>The Physical Security (PS) controls are performed by Microsoft Azure which, as mentioned in the system description, and are carved out within the Azure DevOps SOC 2 report.</p> <p>Azure DevOps does not own, operate or manage PS controls and criteria anticipated by C5.</p>	<p>No exceptions noted.</p>

C5 Criteria	Azure DevOps Activity	Test Result
<p>The security measures are designed to detect and prevent unauthorised access so that the information security of the cloud service is not compromised.</p>	<p>The outer doors, windows and other construction elements reach a level appropriate to the security requirements and withstand a burglary attempt for at least 10 minutes.</p> <p>The surrounding wall constructions as well as the locking mechanisms meet the associated requirements.</p>	
<p>PS-04 At access points to premises and buildings related to the cloud service provided, physical access controls are set up in accordance with the Cloud Service Provider's security requirements (cf. PS-01 Security Concept) to prevent unauthorised access.</p> <p>Access controls are supported by an access control system.</p> <p>The requirements for the access control system are documented, communicated and provided in a policy or concept in accordance with SP-01 and include the following aspects:</p> <ul style="list-style-type: none"> • Specified procedure for the granting and revoking of access authorisations (cf. IDM-02) based on the principle of least authorisation ("least-privilege-principle") and 	<p>This C5 criteria is not applicable to Azure DevOps due to the following reasons:</p> <p>The Physical Security (PS) controls are performed by Microsoft Azure which, as mentioned in the system description, and are carved out within the Azure DevOps SOC 2 report.</p> <p>Azure DevOps does not own, operate or manage PS controls and criteria anticipated by C5.</p>	<p>No exceptions noted.</p>

C5 Criteria	Azure DevOps Activity	Test Result
<p>as necessary for the performance of tasks ("need-to-know-principle");</p> <ul style="list-style-type: none"> • Automatic revocation of access authorisations if they have not been used for a period of 2 month • Automatic withdrawal of access authorisations if they have not been used for a period of 6 months; • Two-factor authentication for access to areas hosting system components that process cloud customer information; • Visitors and external personnel are tracked individually by the access control during their work in the premises and buildings, identified as such (e.g. by visible wearing of a visitor pass) and supervised during their stay; and • Existence and nature of access logging that enables the Cloud Service Provider, in the sense of an effectiveness audit, to check whether only defined personnel have entered the premises and buildings related to the cloud service provided. 		
<p>PS-05 Premises and buildings related to the cloud service provided are protected from fire and smoke by structural, technical and organisational measures that meet the security requirements of the Cloud Service Provider (cf. PS-01 Security Concept) and include the following aspects:</p> <p>a) Structural Measures:</p>	<p>This C5 criteria is not applicable to Azure DevOps due to the following reasons:</p> <p>The Physical Security (PS) controls are performed by Microsoft Azure which, as mentioned in the system description, and are carved out within the Azure DevOps SOC 2 report.</p> <p>Azure DevOps does not own, operate or manage PS controls and criteria anticipated by C5.</p>	<p>No exceptions noted.</p>

C5 Criteria	Azure DevOps Activity	Test Result
<p>Establishment of fire sections with a fire resistance duration of at least 90 minutes for all structural parts</p> <p>b) Technical Measures:</p> <ul style="list-style-type: none"> • Early fire detection with automatic voltage release. The monitored areas are sufficiently fragmented to ensure that the prevention of the spread of incipient fires is proportionate to the maintenance of the availability of the cloud service provided; • Extinguishing system or oxygen reduction; and • Fire alarm system with reporting to the local fire department. <p>c) Organisational Measures:</p> <ul style="list-style-type: none"> • Regular fire protection inspections to check compliance with fire protection requirements; and • Regular fire protection exercises. 		
<p>PS-06 Measures to prevent the failure of the technical supply facilities required for the operation of system components with which information from cloud customers is processed, are documented and set up in accordance with the security requirements of the Cloud Service Provider (cf. PS-01 Security Concept) with respect to the following aspects:</p> <p>a) Operational redundancy (N+1) in power and cooling supply</p>	<p>This C5 criteria is not applicable to Azure DevOps due to the following reasons:</p> <p>The Physical Security (PS) controls are performed by Microsoft Azure which, as mentioned in the system description, and are carved out within the Azure DevOps SOC 2 report.</p> <p>Azure DevOps does not own, operate or manage PS controls and criteria anticipated by C5.</p>	<p>No exceptions noted.</p>

C5 Criteria	Azure DevOps Activity	Test Result
<p>b) Use of appropriately sized uninterruptible power supplies (UPS) and emergency power systems (NEA), designed to ensure that all data remains undamaged in the event of a power failure. The functionality of UPS and NEA is checked at least annually by suitable tests and exercises (cf. BCM-04 - Verification, updating and testing of business continuity).</p> <p>c) Maintenance (servicing, inspection, repair) of the utilities in accordance with the manufacturer's recommendations.</p> <p>d) Protection of power supply and telecommunications lines against interruption, interference, damage and eavesdropping. The protection is checked regularly, but at least every two years, as well as in case of suspected manipulation by qualified personnel regarding the following aspects:</p> <ul style="list-style-type: none"> • Traces of violent attempts to open closed distributors; • Up-to-datedness of the documentation in the distribution list; • Conformity of the actual wiring and patching with the documentation; • The short-circuits and earthing of unneeded cables are intact; and • Impermissible installations and modifications. 		

C5 Criteria	Azure DevOps Activity	Test Result
<p>PS-07 The operating parameters of the technical utilities (cf. PS-06) and the environmental parameters of the premises and buildings related to the cloud service provided are monitored and controlled in accordance with the security requirements of the Cloud Service Provider (cf. PS-01 Security Concept). When the permitted control range is exceeded, the responsible departments of the Cloud-Provider are automatically informed in order to promptly initiate the necessary measures for return to the control range.</p>	<p>This C5 criteria is not applicable to Azure DevOps due to the following reasons:</p> <p>The Physical Security (PS) controls are performed by Microsoft Azure which, as mentioned in the system description, and are carved out within the Azure DevOps SOC 2 report.</p> <p>Azure DevOps does not own, operate or manage PS controls and criteria anticipated by C5.</p>	<p>No exceptions noted.</p>

OPS: Operations

Control Objective 5.6: Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.

C5 Criteria	Azure DevOps Activity	Test Result
<p>OPS-01 The planning of capacities and resources (personnel and IT resources) follows an established procedure in order to avoid possible capacity bottlenecks. The procedures include forecasting future capacity requirements in order to identify usage trends and manage system overload.</p> <p>Cloud Service Providers take appropriate measures to ensure that they continue to meet the requirements agreed with cloud customers for the provision of the cloud service in the event of capacity bottlenecks or outages regarding personnel and IT resources, in particular those relating to the dedicated use of system components, in accordance with the respective agreements.</p>	<p>BC - 5. Management has established monitoring mechanisms to address capacity issues in a timely manner.</p> <p>SOC2 - 2. The service maintains an inventory of key information assets. Procedures are established to review usage of key information assets on at least an annual basis.</p>	No exceptions noted.
<p>OPS-02 Technical and organisational safeguards for the monitoring and provisioning and de-provisioning of cloud services are defined. Thus, the Cloud Service Provider ensures that resources are provided and/or services are rendered according to the contractual agreements and that compliance with the service level agreements is ensured.</p>	<p>SOC2 - 6. The service maintains and notifies customers of potential changes, and security and availability type of events that may impact the service, through an online Service Dashboard. Changes to the security commitments and security obligations of the service's customers are updated on the Azure DevOps website in a timely manner.</p> <p>LA - 1. External access to customer data stored in the service requires authentication.</p> <p>LA - 5. Customer-configured authorization settings can be set to further restrict authentication methods.</p> <p>PI - 2. Azure DevOps management reviews portal performance periodically to evaluate compliance with customer SLA requirements.</p>	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
	VM - 7. The availability of the service is monitored through third-party and internal tools, and the status is communicated through a Service Dashboard.	
OPS-03 Depending on the capabilities of the respective service model, the cloud customer can control and monitor the allocation of the system resources assigned to the customer for administration/use in order to avoid overcrowding of resources and to achieve sufficient performance.	This C5 criteria is not applicable as Azure DevOps is a SaaS offering and none of the in-scope features provide customers the ability to alter capacity.	No exceptions noted.
OPS-04 Policies and instructions with specifications for protection against malware are documented, communicated, and provided in accordance with SP-01 with respect to the following aspects: <ul style="list-style-type: none"> • Use of system-specific protection mechanisms; • Operating protection programs on system components under the responsibility of the Cloud Service Provider that are used to provide the cloud service in the production environment; and • Operation of protection programs for employees' terminal equipment. 	C5 - 1. Standard Operating Procedures (SOPs), that define the procedures required to operate and maintain the Service environment, have been established and communicated to employees. SOPs are reviewed and approved annually by appropriate management. IS - 1. Microsoft has documented and communicated a security policy that defines the information security rules and requirements for the Azure DevOps environment.	No exceptions noted.
OPS-05 System components under the Cloud Service Provider's responsibility that are used to deploy the cloud service in the production environment are configured with malware protection according to the policies and instructions. If protection programs are set up with signature and behaviour-based	VM - 1. Production and supporting infrastructure are configured to log and collect security events. VM - 3. A monitoring system is implemented on production and supporting infrastructure to monitor the service for potential malicious activity and intrusion past service trust boundaries.	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
malware detection and removal, these protection programs are updated at least daily.		
<p>OPS-06 Policies and instructions for data backup and recovery are documented, communicated and provided in accordance with SP-01 regarding the following aspects.</p> <ul style="list-style-type: none"> • The extent and frequency of data backups and the duration of data retention are consistent with the contractual agreements with the cloud customers and the Cloud Service Provider's operational continuity requirements for Recovery Time Objective (RTO) and Recovery Point Objective (RPO); • Data is backed up in encrypted, state-of-the-art form; • Access to the backed-up data and the execution of restores is performed only by authorised persons; and • Tests of recovery procedures (cf. OPS-08). 	<p>C5 - 1. Standard Operating Procedures (SOPs), that define the procedures required to operate and maintain the Service environment, have been established and communicated to employees. SOPs are reviewed and approved annually by appropriate management.</p> <p>DS - 5. Backups of key service components are performed regularly and stored in fault tolerant (isolated) facilities. Backups are monitored and backup errors are investigated and followed-up on appropriately.</p> <p>DS - 6. Critical Azure DevOps components are designed with redundancy to sustain isolated faults and minimize disruptions to customer services.</p> <p>DS - 7. Customer data is automatically replicated to minimize isolated faults. Customers are able to determine geographical regions of the data processing and storage, including data backups.</p> <p>DS - 8. Upon termination of a customer account, the customer data is removed based upon the stipulated retention and removal timelines.</p> <p>OA - 1. Administrative access to the service is controlled through defined interfaces that require authentication using AD credentials.</p>	No exceptions noted.
<p>OPS-07 The execution of data backups is monitored by technical and organisational measures. Malfunctions are investigated by qualified staff and rectified promptly to ensure compliance with contractual obligations to cloud customers or the Cloud Service Provider's business requirements regarding the scope and frequency of data backup and the duration of storage.</p>	<p>DS - 5. Backups of key service components are performed regularly and stored in fault tolerant (isolated) facilities. Backups are monitored and backup errors are investigated and followed-up on appropriately.</p>	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
<p>OPS-08 Restore procedures are tested regularly, at least annually. The tests allow an assessment to be made as to whether the contractual agreements as well as the specifications for the maximum tolerable downtime (Recovery Time Objective, RTO) and the maximum permissible data loss (Recovery Point Objective, RPO) are adhered to (cf. BCM-02).</p> <p>Deviations from the specifications are reported to the responsible personnel or system components so that these can promptly assess the deviations and initiate the necessary actions.</p>	<p>DS - 5. Backups of key service components are performed regularly and stored in fault tolerant (isolated) facilities. Backups are monitored and backup errors are investigated and followed-up on appropriately.</p> <p>BC - 2. Business Continuity Plans (BCP) are documented and published for critical services, which provide roles and responsibilities and detailed procedures for recovery and reconstitution of systems to a known state per defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Plans are reviewed on an annual basis, at a minimum.</p> <p>BC - 4. The BCP team conducts testing of the business continuity and disaster recovery plans at least annually. Issues identified during testing are resolved during the exercises and plans are updated accordingly.</p>	No exceptions noted.
<p>OPS-09 The Cloud Service Provider transfers data to be backed up to a remote location or transports these on backup media to a remote location. If the data backup is transmitted to the remote location via a network, the data backup or the transmission of the data takes place in an encrypted form that corresponds to the state-of-the-art. The distance to the main site is chosen after sufficient consideration of the factors recovery times and impact of disasters on both sites. The physical and environmental security measures at the remote site are at the same level as at the main site.</p>	<p>DS - 2. Customer data communicated through service interfaces is encrypted during transmission over external networks.</p> <p>DS - 3. Internal communication between key components where customer data is transmitted / involved is secured using SSL or equivalent mechanism(s).</p> <p>DS - 5. Backups of key service components are performed regularly and stored in fault tolerant (isolated) facilities. Backups are monitored and backup errors are investigated and followed-up on appropriately.</p> <p>DS - 6. Critical Azure DevOps components are designed with redundancy to sustain isolated faults and minimize disruptions to customer services.</p> <p>DS - 7. Customer data is automatically replicated to minimize isolated faults. Customers are able to determine geographical regions of the data processing and storage, including data backups.</p>	No exceptions noted.
<p>OPS-10 The Cloud Service Provider has established policies and instructions that govern the logging and monitoring of events</p>	<p>C5 - 1. Standard Operating Procedures (SOPs), that define the procedures required to operate and maintain the Service environment, have been</p>	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
<p>on system components within its area of responsibility. These policies and instructions are documented, communicated and provided according to SP-01 with respect to the following aspects:</p> <ul style="list-style-type: none"> • Definition of events that could lead to a violation of the protection goals; • Specifications for activating, stopping and pausing the various logs; • Information regarding the purpose and retention period of the logs. • Define roles and responsibilities for setting up and monitoring logging; • Time synchronisation of system components; and • Compliance with legal and regulatory frameworks. 	<p>established and communicated to employees. SOPs are reviewed and approved annually by appropriate management.</p> <p>C5 - 2. Availability of logging and monitoring software is monitored by internal tools on a continuous basis, and responsible personnel is notified in case of any failure.</p> <p>C5 - 3. Microsoft Azure DevOps components are configured to use Coordinated Universal Time (UTC) time and the clocks are synchronized with the domain controller server.</p> <p>VM - 1. Production and supporting infrastructure are configured to log and collect security events.</p> <p>VM - 2. Administrator activity is logged.</p> <p>VM - 4. Procedures have been established to investigate and respond to the malicious events detected by the monitoring system for timely resolution.</p> <p>VM - 7. The availability of the service is monitored through third-party and internal tools, and the status is communicated through a Service Dashboard.</p>	
<p>OPS-11 Policies and instructions for the secure handling of metadata (usage data) are documented, communicated and provided according to SP-01 with regard to the following aspects:</p> <ul style="list-style-type: none"> • Metadata is collected and used solely for billing, incident management and security incident management purposes; • Exclusively anonymous metadata to deploy and enhance the cloud service so that no conclusions can be drawn about the cloud customer or user; 	<p>C5 - 1. Standard Operating Procedures (SOPs), that define the procedures required to operate and maintain the Service environment, have been established and communicated to employees. SOPs are reviewed and approved annually by appropriate management.</p> <p>C5 - 4. Customer metadata is collected, retained, and removed based on the documented procedures.</p>	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
<ul style="list-style-type: none"> • No commercial use; • Storage for a fixed period reasonably related to the purposes of the collection; • Immediate deletion if the purposes of the collection are fulfilled and further storage is no longer necessary. • Provision to cloud customers according to contractual agreements. 		
<p>OPS-12 The requirements for the logging and monitoring of events and for the secure handling of metadata are implemented by technically supported procedures with regard to the following restrictions:</p> <ul style="list-style-type: none"> • Access only for authorised users and systems; • Retention for the specified period; and • Deletion when further retention is no longer necessary for the purpose of collection. 	<p>C5 - 2. Availability of logging and monitoring software is monitored by internal tools on a continuous basis, and responsible personnel is notified in case of any failure.</p> <p>VM - 1. Production and supporting infrastructure are configured to log and collect security events.</p> <p>VM - 2. Administrator activity is logged.</p> <p>VM - 4. Procedures have been established to investigate and respond to the malicious events detected by the monitoring system for timely resolution.</p> <p>VM - 7. The availability of the service is monitored through third-party and internal tools, and the status is communicated through a Service Dashboard.</p> <p>C5 - 4. Customer metadata is collected, retained, and removed based on the documented procedures.</p>	No exceptions noted.
<p>OPS-13 The logging data is automatically monitored for events that may violate the protection goals in accordance with the logging and monitoring requirements. This also includes the detection of relationships between events (event correlation).</p>	<p>VM - 1. Production and supporting infrastructure are configured to log and collect security events.</p> <p>VM - 2. Administrator activity is logged.</p> <p>VM - 3. A monitoring system is implemented on production and supporting infrastructure to monitor the service for potential malicious activity and intrusion past service trust boundaries.</p>	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
Identified events are automatically reported to the appropriate departments for prompt evaluation and action.	<p>VM - 4. Procedures have been established to investigate and respond to the malicious events detected by the monitoring system for timely resolution.</p> <p>IM - 3. The Service Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures.</p> <p>IM - 4. Incident post-mortem activities are conducted for high severity incidents impacting the service environment.</p>	
<p>OPS-14 The Cloud Service Provider retains the generated log data and keeps these in an appropriate, unchangeable and aggregated form, regardless of the source of such data, so that a central, authorised evaluation of the data is possible. Log data is deleted if it is no longer required for the purpose for which they were collected.</p> <p>Between logging servers and the assets to be logged, authentication takes place to protect the integrity and authenticity of the information transmitted and stored. The transfer takes place using state-of-the-art encryption or a dedicated administration network (out-of-band management).</p>	<p>C5 - 5. Logging servers are required to authenticate over encrypted channel to access logs generated within the production environment. Access to logging and monitoring infrastructure is restricted to authorized personnel.</p> <p>DS - 3. Internal communication between key components where customer data is transmitted / involved is secured using SSL or equivalent mechanism(s).</p> <p>VM - 1. Production and supporting infrastructure are configured to log and collect security events.</p> <p>VM - 2. Administrator activity is logged.</p>	No exceptions noted.
<p>OPS-15 The log data generated allows an unambiguous identification of user accesses at tenant level to support (forensic) analysis in the event of a security incident.</p> <p>Interfaces are available to conduct forensic analyses and perform backups of infrastructure components and their network communication.</p>	<p>C5 - 6. Microsoft Azure DevOps has established forensic procedures to support potential legal action after an information security incident.</p> <p>VM - 2. Administrator activity is logged.</p>	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
<p>OPS-16 Access to system components for logging and monitoring in the Cloud Service Provider's area of responsibility is restricted to authorised users. Changes to the configuration are made in accordance with the applicable policies (cf. DEV-03).</p>	<p>C5 - 5. Logging servers are required to authenticate over encrypted channel to access logs generated within the production environment. Access to logging and monitoring infrastructure is restricted to authorized personnel.</p> <p>CM - 2. Key stakeholders approve changes prior to release into production based on documented change management procedures.</p> <p>CM - 4. Software releases and configuration changes are tested based on established criteria prior to production implementation.</p> <p>CM - 5. Implemented changes are reviewed for adherence to established procedures prior to closure. Changes are rolled back to their previous state in case of errors or security concerns.</p>	No exceptions noted.
<p>OPS-17 The Cloud Service Provider monitors the system components for logging and monitoring in its area of responsibility. Failures are automatically and promptly reported to the Cloud Service Provider's responsible departments so that these can assess the failures and take required action.</p>	<p>C5 - 2. Availability of logging and monitoring software is monitored by internal tools on a continuous basis, and responsible personnel is notified in case of any failure.</p>	No exceptions noted.
<p>OPS-18 Guidelines and instructions with technical and organisational measures are documented, communicated and provided in accordance with SP-01 to ensure the timely identification and addressing of vulnerabilities in the system components used to provide the cloud service. These guidelines and instructions contain specifications regarding the following aspects:</p> <ul style="list-style-type: none"> • Regular identification of vulnerabilities; 	<p>C5 - 1. Standard Operating Procedures (SOPs), that define the procedures required to operate and maintain the Service environment, have been established and communicated to employees. SOPs are reviewed and approved annually by appropriate management.</p> <p>VM - 5. Procedures are established to evaluate and implement Microsoft released patches to service components.</p> <p>VM - 6. Procedures are established to monitor production and supporting infrastructure for known security vulnerabilities. Identified security vulnerabilities are remediated.</p>	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
<ul style="list-style-type: none"> • Assessment of the severity of identified vulnerabilities; • Prioritisation and implementation of actions to promptly remediate or mitigate identified vulnerabilities based on severity and according to defined timelines; and • Handling of system components for which no measures are initiated for the timely remediation or mitigation of vulnerabilities. 		
<p>OPS-19 The Cloud Service Provider has penetration tests carried out by qualified internal personnel or external service providers at least once a year. The penetration tests are carried out according to a documented test methodology and include the system components relevant to the provision of the cloud service in the area of responsibility of the Cloud Service Provider, which have been identified as such in a risk analysis.</p> <p>The Cloud Service Provider assess the severity of the findings made in penetration tests according to defined criteria.</p> <p>For findings with medium or high criticality regarding the confidentiality, integrity or availability of the cloud service, actions must be taken within defined time windows for prompt remediation or mitigation.</p>	<p>VM - 8. Penetration testing is performed on critical infrastructure components at least annually. Findings are documented, tracked and remediated.</p>	No exceptions noted.
<p>OPS-20 The Cloud Service Provider regularly measures, analyses and assesses the procedures with which vulnerabilities and</p>	<p>C5 - 1. Standard Operating Procedures (SOPs), that define the procedures required to operate and maintain the Service environment, have been</p>	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
<p>incidents are handled to verify their continued suitability, appropriateness and effectiveness.</p> <p>Results are evaluated at least quarterly by accountable departments at the Cloud Service Provider to initiate continuous improvement actions and to verify their effectiveness.</p>	<p>established and communicated to employees. SOPs are reviewed and approved annually by appropriate management.</p> <p>IM - 1. An incident management framework is established and communicated with defined processes, roles and responsibilities for the detection, escalation and response of incidents.</p> <p>VM - 6. Procedures are established to monitor production and supporting infrastructure for known security vulnerabilities. Identified security vulnerabilities are remediated.</p> <p>SOC2 - 18. Microsoft Azure DevOps performs an annual risk assessment that covers security, continuity, and operational risks. As part of this process, threats to security are identified and risks from these threats are formally assessed.</p> <p>D&T Note:</p> <p>Azure DevOps reviews vulnerability and incident management procedures annually rather than quarterly. Management reviews the implementation of these procedures as part of their internal monitoring and changes can be made as often as needed, supporting continuous improvement of the processes and procedures. Thus, we can conclude that the design of controls is appropriate to meet the C5 Objective 5.6.</p>	<p>No exceptions noted.</p>
<p>OPS-21 The Cloud Service Provider periodically informs the cloud customer on the status of incidents affecting the cloud customer, or, where appropriate and necessary, involve the customer in the resolution, in a manner consistent with the contractual agreements.</p> <p>As soon as an incident has been resolved from the Cloud Service Provider's perspective, the cloud customer is informed according to the contractual agreements, about the actions taken.</p>	<p>IM - 1. An incident management framework is established and communicated with defined processes, roles and responsibilities for the detection, escalation and response of incidents.</p> <p>SOC2 - 3. The service maintains a customer support website that describes the process for customers and other external users to inform about potential security issues and submitting complaints. Reported issues are reviewed and addressed per documented incident management procedures.</p> <p>SOC2 - 6. The service maintains and notifies customers of potential changes, and security and availability type of events that may impact the service, through an online Service Dashboard. Changes to the security commitments and security obligations of the service's customers are updated on the Azure DevOps website in a timely manner.</p>	<p>No exceptions noted.</p>

C5 Criteria	Azure DevOps Activity	Test Result
<p>OPS-22 System components in the area of responsibility of the Cloud Service Provider for the provision of the cloud service are automatically checked for known vulnerabilities at least once a month in accordance with the policies for handling vulnerabilities (cf. OPS-18), the severity is assessed in accordance with defined criteria and measures for timely remediation or mitigation are initiated within defined time windows.</p>	<p>VM - 5. Procedures are established to evaluate and implement Microsoft released patches to service components.</p> <p>VM - 6. Procedures are established to monitor production and supporting infrastructure for known security vulnerabilities. Identified security vulnerabilities are remediated.</p> <p>D&T Note:</p> <p>Azure DevOps performs quarterly vulnerability scans on its production environment rather than the monthly scans. Additionally, the production environment is continuously monitored for security and baseline configurations. Thus, we can conclude that the design is appropriate to meet the C5 Objective 5.6.</p>	No exceptions noted.
<p>OPS-23 System components in the production environment used to provide the cloud service under the Cloud Service Provider's responsibility are hardened according to generally accepted industry standards. The hardening requirements for each system component are documented.</p> <p>If non-modifiable ("immutable") images are used, compliance with the hardening specifications as defined in the hardening requirements is checked upon creation of the images. Configuration and log files regarding the continuous availability of the images are retained.</p>	<p>SOC2 - 12. The security baselines are refreshed for Azure DevOps on a periodic basis.</p>	No exceptions noted.
<p>OPS-24 Cloud customer data stored and processed on shared virtual and physical resources is securely and strictly separated according to a documented approach based</p>	<p>SOC2 - 18. Microsoft Azure DevOps performs an annual risk assessment that covers security, continuity, and operational risks. As part of this process, threats to security are identified and risks from these threats are formally assessed.</p>	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
on OIS-07 risk analysis to ensure the confidentiality and integrity of this data.	LA - 3. Logical segregation is implemented to restrict unauthorized access to other customer tenants.	

IDM: Identity and Access Management

Control Objective 5.7: Secure the authorisation and authentication of users of the Cloud Service Provider (typically privileged users) to prevent unauthorised access.

C5 Criteria	Azure DevOps Activity	Test Result
<p>IDM-01 A role and rights concept based on the business and security requirements of the Cloud Service Provider as well as a policy for managing user accounts and access rights for internal and external employees of the Cloud Service Provider and system components that have a role in automated authorisation processes of the Cloud Service Provider are documented, communicated and made available according to SP-01:</p> <ul style="list-style-type: none"> • Assignment of unique usernames; • Granting and modifying user accounts and access rights based on the "least-privilege-principle" and the "need-to-know" principle; • Segregation of duties between operational and monitoring functions ("Segregation of Duties"); 	<p>C5 - 1. Standard Operating Procedures (SOPs), that define the procedures required to operate and maintain the Service environment, have been established and communicated to employees. SOPs are reviewed and approved annually by appropriate management.</p> <p>OA - 1. Administrative access to the service is controlled through defined interfaces that require authentication using AD credentials.</p> <p>OA - 2. Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning access to employees, contractors, and service providers to specific applications or information resources.</p> <p>OA - 4. Password complexity standards are defined and enforced for Azure DevOps personnel credentials.</p> <p>OA - 5. Access privileges are reviewed quarterly to determine if access rights are commensurate to the user's job duties. Access is modified based on the results of the reviews.</p> <p>OA - 6. Procedures are established for granting temporary access for personnel to customer data and applications upon appropriate approval.</p>	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
<ul style="list-style-type: none"> • Segregation of duties between managing, approving and assigning user accounts and access rights; • Approval by authorised individual(s) or system(s) for granting or modifying user accounts and access rights before data of the cloud customer or system components used to provision the cloud service can be accessed; • Regular review of assigned user accounts and access rights; • Blocking and removing access accounts in the event of inactivity; • Time-based or event-driven removal or adjustment of access rights in the event of changes to job responsibility; • Two-factor or multi-factor authentication for users with privileged access; • Requirements for the approval and documentation of the management of user accounts and access rights. 	<p>OA - 9. Production domain-level user accounts are disabled after a stipulated period of inactivity.</p> <p>OA - 10. Access to production resources requires the use of a Secure Admin Workstation (SAW) which requires MFA for access. SAWs are hardened and secured devices with restricted access.</p> <p>LA - 1. External access to customer data stored in the service requires authentication.</p> <p>LA - 5. Customer-configured authorization settings can be set to further restrict authentication methods.</p>	
<p>IDM-02 Specified procedures for granting and modifying user accounts and access rights for internal and external employees of the Cloud Service Provider as well as for system components involved in automated authorisation processes of the Cloud Service Provider ensure compliance with the role and rights concept as well as the policy for managing user accounts and access rights.</p>	<p>OA - 1. Administrative access to the service is controlled through defined interfaces that require authentication using AD credentials.</p> <p>OA - 2. Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning access to employees, contractors, and service providers to specific applications or information resources.</p> <p>OA - 3. Procedures are in place to disable accounts on a timely basis, upon the user's termination.</p>	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
	<p>OA - 5. Access privileges are reviewed quarterly to determine if access rights are commensurate to the user's job duties. Access is modified based on the results of the reviews.</p> <p>OA - 6. Procedures are established for granting temporary access for personnel to customer data and applications upon appropriate approval.</p> <p>OA - 8. Alerts are generated when a break-glass account is used to access production environment.</p> <p>OA - 9. Production domain-level user accounts are disabled after a stipulated period of inactivity.</p> <p>OA - 10. Access to production resources requires the use of a Secure Admin Workstation (SAW) which requires MFA for access. SAWs are hardened and secured devices with restricted access.</p> <p>SOC2 - 17. Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within Azure DevOps environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Legal and Corporate Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements.</p> <p>C5 - 1. Standard Operating Procedures (SOPs), that define the procedures required to operate and maintain the Service environment, have been established and communicated to employees. SOPs are reviewed and approved annually by appropriate management.</p>	
IDM-03 User accounts of internal and external employees of the Cloud Service Provider as well as for system components involved in automated authorisation processes of the Cloud Service Provider are automatically locked if they have not been used for a period of two months. Approval from authorised personnel or system	<p>OA - 1. Administrative access to the service is controlled through defined interfaces that require authentication using AD credentials.</p> <p>OA - 2. Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning access to employees, contractors, and service providers to specific applications or information resources.</p> <p>OA - 3. Procedures are in place to disable accounts on a timely basis, upon the user's termination.</p>	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
<p>components are required to unlock these accounts.</p> <p>Locked user accounts are automatically revoked after six months. After revocation, the procedure for granting user accounts and access rights (cf. IDM-02) must be repeated.</p>	<p>OA - 4. Password complexity standards are defined and enforced for Azure DevOps personnel credentials.</p> <p>OA - 5. Access privileges are reviewed quarterly to determine if access rights are commensurate to the user's job duties. Access is modified based on the results of the reviews.</p> <p>OA - 6. Procedures are established for granting temporary access for personnel to customer data and applications upon appropriate approval.</p> <p>OA - 9. Production domain-level user accounts are disabled after a stipulated period of inactivity.</p> <p>OA - 10. Access to production resources requires the use of a Secure Admin Workstation (SAW) which requires MFA for access. SAWs are hardened and secured devices with restricted access.</p>	
<p>IDM-04 Access rights are promptly revoked if the job responsibilities of the Cloud Service Provider's internal or external staff or the tasks of system components involved in the Cloud Service Provider's automated authorisation processes change. Privileged access rights are adjusted or revoked within 48 hours after the change taking effect. All other access rights are adjusted or revoked within 14 days. After revocation, the procedure for granting user accounts and access rights (cf. IDM-02) must be repeated.</p>	<p>OA - 1. Administrative access to the service is controlled through defined interfaces that require authentication using AD credentials.</p> <p>OA - 2. Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning access to employees, contractors, and service providers to specific applications or information resources.</p> <p>OA - 3. Procedures are in place to disable accounts on a timely basis, upon the user's termination.</p> <p>OA - 5. Access privileges are reviewed quarterly to determine if access rights are commensurate to the user's job duties. Access is modified based on the results of the reviews.</p> <p>OA - 6. Procedures are established for granting temporary access for personnel to customer data and applications upon appropriate approval.</p> <p>OA - 9. Production domain-level user accounts are disabled after a stipulated period of inactivity.</p> <p>OA - 10. Access to production resources requires the use of a Secure Admin Workstation (SAW) which requires MFA for access. SAWs are hardened and secured devices with restricted access.</p>	<p>No exceptions noted.</p>

C5 Criteria	Azure DevOps Activity	Test Result
<p>IDM-05 Access rights of internal and external employees of the Cloud Service Provider as well as of system components that play a role in automated authorisation processes of the Cloud Service Provider are reviewed at least once a year to ensure that they still correspond to the actual area of use. The review is carried out by authorised persons from the Cloud Service Provider's organisational units, who can assess the appropriateness of the assigned access rights based on their knowledge of the task areas of the employees or system components. Identified deviations will be dealt with promptly, but no later than 7 days after their detection, by appropriate modification or withdrawal of the access rights.</p>	<p>OA - 1. Administrative access to the service is controlled through defined interfaces that require authentication using AD credentials.</p> <p>OA - 2. Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning access to employees, contractors, and service providers to specific applications or information resources.</p> <p>OA - 5. Access privileges are reviewed quarterly to determine if access rights are commensurate to the user's job duties. Access is modified based on the results of the reviews.</p> <p>D&T Note:</p> <p>The access revocation based on user access reviews may or may not be completed within 7 days of identification given the time allotted to reviewers to finalize their review of accounts within Azure DevOps. Based on the access reviews, access modifications or withdrawals, if any, are performed as needed. Azure DevOps user access reviews are performed on a quarterly basis rather than on annual basis as noted in the criteria. Thus, we can conclude that the design of controls is appropriate to meet the C5 objective 5.7.</p>	No exceptions noted.
<p>IDM-06 Privileged access rights for internal and external employees as well as technical users of the Cloud Service Provider are assigned and changed in accordance to the policy for managing user accounts and access rights (cf. IDM-01) or a separate specific policy.</p> <p>Privileged access rights are personalised, limited in time according to a risk assessment and assigned as necessary for the execution of tasks ("need-to-know principle"). Technical users are assigned to internal or external employees of the Cloud Service Provider.</p>	<p>OA - 1. Administrative access to the service is controlled through defined interfaces that require authentication using AD credentials.</p> <p>OA - 2. Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning access to employees, contractors, and service providers to specific applications or information resources.</p> <p>OA - 7. Authentication over an encrypted Remote Desktop Connection is used for administrator access to the production environment.</p> <p>OA - 8. Alerts are generated when a break-glass account is used to access production environment.</p> <p>VM - 2. Administrator activity is logged.</p> <p>VM - 4. Procedures have been established to investigate and respond to the malicious events detected by the monitoring system for timely resolution.</p>	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
Activities of users with privileged access rights are logged in order to detect any misuse of privileged access in suspicious cases. The logged information is automatically monitored for defined events that may indicate misuse. When such an event is identified, the responsible personnel are automatically informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken in accordance with HR-04.	SOC2 - 8. Microsoft has defined disciplinary actions for employees and contingent staff that commit a security breach or violate the security policy.	
IDM-07 The cloud customer is informed by the Cloud Service Provider whenever internal or external employees of the Cloud Service Provider read or write to the cloud customer's data processed, stored or transmitted in the cloud service or have accessed it without the prior consent of the cloud customer. The Information is provided whenever data of the cloud customer is/was not encrypted, the encryption is/was disabled for access or the contractual agreements do not explicitly exclude such information. The information contains the cause, time, duration, type and scope of the access. The information is sufficiently detailed to enable subject matter experts of the cloud customer to assess the risks of the access. The information is provided in accordance with the contractual agreements, or within 72 hours after the access.	<p>OA - 6. Procedures are established for granting temporary access for personnel to customer data and applications upon appropriate approval.</p> <p>D&T Note:</p> <p>Azure DevOps personnel can obtain temporary access to customer data for support purposes only after obtaining appropriate approval from the customer. Access to customer data without prior customer approval is prohibited. The remaining criteria are addressed by controls that are designed to meet the C5 objective 5.7.</p>	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
<p>IDM-08 The allocation of authentication information to access system components used to provide the cloud service to internal and external users of the cloud provider and system components that are involved in automated authorisation processes of the cloud provider is done in an orderly manner that ensures the confidentiality of the information. If passwords are used as authentication information, their confidentiality is ensured by the following procedures, as far as technically possible:</p> <ul style="list-style-type: none"> • Users can initially create the password themselves or must change an initial password when logging on to the system component for the first time. An initial password loses its validity after a maximum of 14 days. • When creating passwords, compliance with the password specifications (cf. IDM-09) is enforced as far as technically possible. • The user is informed about changing or resetting the password. • The server-side storage takes place using cryptographically strong hash functions. <p>Deviations are evaluated by means of a risk analysis and mitigating measures derived from this are implemented.</p>	<p>LA - 2. Customer credentials used to access the service meet the applicable password policy requirements.</p> <p>LA - 4. Customer data that is confidential is protected while in storage within the service.</p> <p>DS - 1. Cryptographic certificates, keys, and customer access keys used for communication between the features and other internal components are stored securely and are rotated on a periodic basis.</p> <p>DS - 4. Cryptographic controls are used for information protection within the platform based on the Cryptographic Policy and Key Management procedures.</p> <p>OA - 1. Administrative access to the service is controlled through defined interfaces that require authentication using AD credentials.</p> <p>OA - 4. Password complexity standards are defined and enforced for Azure DevOps personnel credentials.</p> <p>OA - 10. Access to production resources requires the use of a Secure Admin Workstation (SAW) which requires MFA for access. SAWs are hardened and secured devices with restricted access.</p>	<p>No exceptions noted.</p>
<p>IDM-09 System components in the Cloud Service Provider's area of responsibility that are used to provide the cloud service,</p>	<p>OA - 1. Administrative access to the service is controlled through defined interfaces that require authentication using AD credentials.</p>	<p>No exceptions noted.</p>

C5 Criteria	Azure DevOps Activity	Test Result
<p>authenticate users of the Cloud Service Provider's internal and external employees as well as system components that are involved in the Cloud Service Provider's automated authorisation processes. Access to the production environment requires two-factor or multi-factor authentication. Within the production environment, user authentication takes place through passwords, digitally signed certificates or procedures that achieve at least an equivalent level of security. If digitally signed certificates are used, administration is carried out in accordance with the Guideline for Key Management (cf. CRY-01). The password requirements are derived from a risk assessment and documented, communicated and provided in a password policy according to SP-01. Compliance with the requirements is enforced by the configuration of the system components, as far as technically possible.</p>	<p>OA - 4. Password complexity standards are defined and enforced for Azure DevOps personnel credentials.</p> <p>OA - 7. Authentication over an encrypted Remote Desktop Connection is used for administrator access to the production environment.</p> <p>OA - 10. Access to production resources requires the use of a Secure Admin Workstation (SAW) which requires MFA for access. SAWs are hardened and secured devices with restricted access.</p> <p>LA - 2. Customer credentials used to access the service meet the applicable password policy requirements.</p> <p>C5 - 1. Standard Operating Procedures (SOPs), that define the procedures required to operate and maintain the Service environment, have been established and communicated to employees. SOPs are reviewed and approved annually by appropriate management.</p>	

CRY: Cryptography and Key Management

Control Objective 5.8: Ensure appropriate and effective use of cryptography to protect the confidentiality, authenticity or integrity of information.

C5 Criteria	Azure DevOps Activity	Test Result
<p>CRY-01 Policies and instructions with technical and organisational safeguards for encryption procedures and key management are documented, communicated and provided according to SP-01, in which the following aspects are described:</p> <ul style="list-style-type: none">• Usage of strong encryption procedures and secure network protocols that correspond to the state-of-the-art;• Risk-based provisions for the use of encryption which information classification schemes (cf. AM-06) and consider the communication channel, type, strength and quality of the encryption;• Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys; and• Consideration of relevant legal and regulatory obligations and requirements.	<p>C5 - 1. Standard Operating Procedures (SOPs), that define the procedures required to operate and maintain the Service environment, have been established and communicated to employees. SOPs are reviewed and approved annually by appropriate management.</p>	No exceptions noted.
<p>CRY-02 The Cloud Service Provider has established procedures and technical measures for strong encryption and authentication for the transmission of data of cloud customers over public networks.</p>	<p>DS - 2. Customer data communicated through service interfaces is encrypted during transmission over external networks.</p> <p>LA - 1. External access to customer data stored in the service requires authentication.</p> <p>LA - 5. Customer-configured authorization settings can be set to further restrict authentication methods.</p>	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
<p>CRY-03 The Cloud Service Provider has established procedures and technical safeguards to encrypt cloud customers' data during storage. The private keys used for encryption are known only to the cloud customer in accordance with applicable legal and regulatory obligations and requirements. Exceptions follow a specified procedure. The procedures for the use of private keys, including any exceptions, must be contractually agreed with the cloud customer.</p>	<p>DS - 1. Cryptographic certificates, keys, and customer access keys used for communication between the features and other internal components are stored securely and are rotated on a periodic basis.</p> <p>DS - 2. Customer data communicated through service interfaces is encrypted during transmission over external networks.</p> <p>DS - 3. Internal communication between key components where customer data is transmitted / involved is secured using SSL or equivalent mechanism(s).</p> <p>DS - 4. Cryptographic controls are used for information protection within the platform based on the Cryptographic Policy and Key Management procedures.</p> <p>LA - 4. Customer data that is confidential is protected while in storage within the service.</p>	No exceptions noted.
<p>CRY-04 Procedures and technical safeguards for secure key management in the area of responsibility of the Cloud Service Provider include at least the following aspects:</p> <ul style="list-style-type: none"> • Generation of keys for different cryptographic systems and applications; • Issuing and obtaining public-key certificates; • Provisioning and activation of the keys; • Secure storage of keys (separation of key management system from application and middleware level) including description of how authorised users get access; • Changing or updating cryptographic keys including policies defining under which conditions and in which manner the changes and/or updates are to be realised; 	<p>C5 - 1. Standard Operating Procedures (SOPs), that define the procedures required to operate and maintain the Service environment, have been established and communicated to employees. SOPs are reviewed and approved annually by appropriate management.</p> <p>OA - 1. Administrative access to the service is controlled through defined interfaces that require authentication using AD credentials.</p> <p>DS - 1. Cryptographic certificates, keys, and customer access keys used for communication between the features and other internal components are stored securely and are rotated on a periodic basis.</p> <p>DS - 2. Customer data communicated through service interfaces is encrypted during transmission over external networks.</p> <p>DS - 3. Internal communication between key components where customer data is transmitted / involved is secured using SSL or equivalent mechanism(s).</p> <p>DS - 4. Cryptographic controls are used for information protection within the platform based on the Cryptographic Policy and Key Management procedures.</p>	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
<ul style="list-style-type: none"> • Handling of compromised keys; • Withdrawal and deletion of keys; and • If pre-shared keys are used, the specific provisions relating to the safe use of this procedure are specified separately. 		

COS: Communication Security

Control Objective 5.9: Ensure the protection of information in networks and the corresponding information processing systems

C5 Criteria	Azure DevOps Activity	Test Result
<p>COS-01 Based on the results of a risk analysis carried out according to OIS-06, the Cloud Service Provider has implemented technical safeguards which are suitable to promptly detect and respond to network-based attacks on the basis of irregular incoming or outgoing traffic patterns and/or Distributed Denial- of-Service (DDoS) attacks. Data from corresponding technical protection measures implemented is fed into a comprehensive SIEM (Security Information and Event Management) system, so that (counter) measures regarding correlating events can be initiated. The safeguards are documented, communicated and provided in accordance with SP-01.</p>	<p>This C5 criteria is not applicable to Azure DevOps due to the following reasons:</p> <p>Azure is responsible for maintaining controls over protection of the network environment and infrastructure, including perimeter firewalls and restricting access to network devices.</p>	<p>No exceptions noted.</p>

C5 Criteria	Azure DevOps Activity	Test Result
<p>COS-02 Specific security requirements are designed, published and provided for establishing connections within the Cloud Service Provider's network. The security requirements define for the Cloud Service Provider's area of responsibility:</p> <ul style="list-style-type: none"> • in which cases the security zones are to be separated and in which cases cloud customers are to be logically or physically segregated; • which communication relationships and which network and application protocols are permitted in each case; • how the data traffic for administration and monitoring is segregated from each on network level; • which internal, cross-location communication is permitted and; • which cross-network communication is allowed 	<p>This C5 criteria is not applicable to Azure DevOps due to the following reasons:</p> <p>Azure is responsible for maintaining controls over protection of the network environment and infrastructure, including perimeter firewalls and restricting access to network devices.</p>	<p>No exceptions noted.</p>
<p>COS-03 A distinction is made between trusted and untrusted networks. Based on a risk assessment, these are separated into different security zones for internal and external network areas (and DMZ, if applicable). Physical and virtualised network environments are designed and configured to restrict and monitor the established connection to trusted or untrusted networks according to the defined security requirements.</p>	<p>This C5 criteria is not applicable to Azure DevOps due to the following reasons:</p> <p>Azure is responsible for maintaining controls over protection of the network environment and infrastructure, including perimeter firewalls and restricting access to network devices.</p>	<p>No exceptions noted.</p>

C5 Criteria	Azure DevOps Activity	Test Result
<p>The entirety of the conception and configuration undertaken to monitor the connections mentioned is assessed in a risk-oriented manner, at least annually, with regard to the resulting security requirements.</p> <p>Identified vulnerabilities and deviations are subject to risk assessment in accordance with the risk management procedure (cf. OIS-06) and follow-up measures are defined and tracked (cf. OPS-18).</p> <p>At specified intervals, the business justification for using all services, protocols, and ports is reviewed. The review also includes the justifications for compensatory measures for the use of protocols that are considered insecure.</p>		
COS-04 Each network perimeter is controlled by security gateways. The system access authorisation for cross-network access is based on a security assessment based on the requirements of the cloud customers.	<p>This C5 criteria is not applicable to Azure DevOps due to the following reasons:</p> <p>Azure is responsible for maintaining controls over protection of the network environment and infrastructure, including perimeter firewalls and restricting access to network devices.</p>	No exceptions noted.
COS-05 There are separate networks for the administrative management of the infrastructure and for the operation of management consoles. These networks are logically or physically separated from the cloud customer's network and protected from unauthorised access by multi-factor authentication (cf. IDM-09). Networks used by the Cloud Service Provider to migrate or	<p>This C5 criteria is not applicable to Azure DevOps due to the following reasons:</p> <p>Azure is responsible for maintaining controls over protection of the network environment and infrastructure, including perimeter firewalls and restricting access to network devices.</p>	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
create virtual machines are also physically or logically separated from other networks		
COS-06 Data traffic of cloud customers in jointly used network environments is segregated on network level according to a documented concept to ensure the confidentiality and integrity of the data transmitted.	<p>This C5 criteria is not applicable to Azure DevOps due to the following reasons:</p> <p>Azure is responsible for maintaining controls over protection of the network environment and infrastructure, including perimeter firewalls and restricting access to network devices.</p>	No exceptions noted.
COS-07 The documentation of the logical structure of the network used to provision or operate the Cloud Service, is traceable and up-to-date, in order to avoid administrative errors during live operation and to ensure timely recovery in the event of malfunctions in accordance with contractual obligations. The documentation shows how the subnets are allocated and how the network is zoned and segmented. In addition, the geographical locations in which the cloud customers' data is stored are indicated.	<p>This C5 criteria is not applicable to Azure DevOps due to the following reasons:</p> <p>Azure is responsible for maintaining controls over protection of the network environment and infrastructure, including perimeter firewalls and restricting access to network devices.</p>	No exceptions noted.
COS-08 Policies and instructions with technical and organisational safeguards in order to protect the transmission of data against unauthorised interception, manipulation, copying, modification, redirection or destruction are documented, communicated and provided according to SP-01. The policy and instructions establish a reference to the classification of information (cf. AM-06).	<p>This C5 criteria is not applicable to Azure DevOps due to the following reasons:</p> <p>Azure is responsible for maintaining controls over protection of the network environment and infrastructure, including perimeter firewalls and restricting access to network devices.</p>	No exceptions noted.

PI: Portability and Interoperability

Control Objective 5.10: Enable the ability to access the cloud service via other cloud services or IT systems of the cloud customers, to obtain the stored data at the end of the contractual relationship and to securely delete it from the Cloud Service Provider.

C5 Criteria	Azure DevOps Activity	Test Result
<p>PI-01 The cloud service can be accessed by other cloud services or IT systems of cloud customers through documented inbound and outbound interfaces. Further, the interfaces are clearly documented for subject matter experts on how they can be used to retrieve the data.</p> <p>Communication takes place through standardised communication protocols that ensure the confidentiality and integrity of the transmitted information according to its protection requirements. Communication over untrusted networks is encrypted according to CRY-02.</p> <p>The type and scope of the documentation on the interfaces is geared to the needs of the cloud customers' subject matter experts in order to enable the use of these interfaces. The information is maintained in such a way that it is applicable for the cloud service's version which is intended for productive use.</p>	<p>C5 - 7. Azure DevOps has published a standard set of APIs with an ecosystem of tools and libraries on the Azure DevOps Portal.</p> <p>DS - 2. Customer data communicated through service interfaces is encrypted during transmission over external networks.</p> <p>DS - 3. Internal communication between key components where customer data is transmitted / involved is secured using SSL or equivalent mechanism(s).</p>	<p>No exceptions noted.</p>
<p>PI-02 In contractual agreements, the following aspects are defined with regard to the termination of the contractual relationship, insofar as these are applicable to the cloud service:</p>	<p>DS - 8. Upon termination of a customer account, the customer data is removed based upon the stipulated retention and removal timelines.</p> <p>C5 - 1. Standard Operating Procedures (SOPs), that define the procedures required to operate and maintain the Service environment, have been established and communicated to employees. SOPs are reviewed and approved annually by appropriate management.</p>	<p>No exceptions noted.</p>

C5 Criteria	Azure DevOps Activity	Test Result
<ul style="list-style-type: none"> • Type, scope and format of the data the Cloud Service Provider provides to the cloud customer; • Definition of the timeframe, within which the Cloud Service Provider makes the data available to the cloud customer; • Definition of the point in time as of which the Cloud Service Provider makes the data inaccessible to the cloud customer and deletes these; and • The cloud customers' responsibilities and obligations to cooperate for the provision of the data. <p>The definitions are based on the needs of subject matter experts of potential customers who assess the suitability of the cloud service with regard to a dependency on the Cloud Service Provider as well as legal and regulatory requirements.</p>	<p>C5 - 13. Customer data is accessible within agreed upon services in data formats compatible with providing those services.</p>	
<p>PI-03 The Cloud Service Provider's procedures for deleting the cloud customers' data upon termination of the contractual relationship ensure compliance with the contractual agreements (cf. PI-02).</p> <p>The deletion includes data in the cloud customer's environment, metadata and data stored in the data backups.</p> <p>The deletion procedures prevent recovery by forensic means.</p>	<p>DS - 8. Upon termination of a customer account, the customer data is removed based upon the stipulated retention and removal timelines.</p> <p>C5 - 4. Customer metadata is collected, retained, and removed based on the documented procedures.</p>	<p>No exceptions noted.</p>

DEV: Procurement, Development and Modification of Information Systems

Control Objective 5.11: Ensure information security in the development cycle of information systems.

C5 Criteria	Azure DevOps Activity	Test Result
<p>DEV-01 Policies and instructions with technical and organisational measures for the secure development of the cloud service are documented, communicated and provided in accordance with SP-01.</p> <p>The policies and instructions contain guidelines for the entire life cycle of the cloud service and are based on recognised standards and methods with regard to the following aspects:</p> <ul style="list-style-type: none"> • Security in Software Development (Requirements, Design, Implementation, Testing and Verification); • Security in software deployment (including continuous delivery); and • Security in operation (reaction to identified faults and vulnerabilities). 	<p>C5 - 1. Standard Operating Procedures (SOPs), that define the procedures required to operate and maintain the Service environment, have been established and communicated to employees. SOPs are reviewed and approved annually by appropriate management.</p> <p>CM - 1. Procedures for managing different types of changes to the features are documented and communicated.</p> <p>DS - 4. Cryptographic controls are used for information protection within the platform based on the Cryptographic Policy and Key Management procedures.</p> <p>SDL - 1. Development of new features and changes to existing features follow a defined approach based on the Microsoft Secure Development Lifecycle (SDL) methodology.</p> <p>SDL - 2. Applicable operational security and internal control requirements are documented and approved for Azure DevOps.</p> <p>SDL - 4. Separate environments, outside of production, are established for the purpose of developing and testing changes. Production data is not replicated in test or development environments.</p> <p>SDL - 6. A security review of releases is performed on a periodic basis by designated security personnel within Azure DevOps.</p> <p>SDL - 7. Source code builds are scanned for malware prior to release to production.</p> <p>SOC2 - 12. The security baselines are refreshed for Azure DevOps on a periodic basis.</p>	<p>No exceptions noted.</p>
<p>DEV-02 In the case of outsourced development of the cloud service (or individual system components), specifications regarding the following aspects</p>	<p>Not Applicable as Microsoft Azure DevOps does not outsource development and testing of its services.</p>	<p>No exceptions noted.</p>

C5 Criteria	Azure DevOps Activity	Test Result
<p>are contractually agreed between the Cloud Service Provider and the outsourced development contractor:</p> <ul style="list-style-type: none"> • Security in software development (requirements, design, implementation, tests and verifications) in accordance with recognised standards and methods; • Acceptance testing of the quality of the services provided in accordance with the agreed functional and non-functional requirements; and • Providing evidence that sufficient verifications have been carried out to rule out the existence of known vulnerabilities. 		
<p>DEV-03 Policies and instructions with technical and organisational safeguards for change management of system components of the cloud service within the scope of software deployment are documented, communicated and provided according to SP-01 with regard to the following aspects:</p> <ul style="list-style-type: none"> • Criteria for risk assessment, categorisation and prioritisation of changes and related requirements for the type and scope of testing to be performed, and necessary approvals for the development/implementation of the change and releases for deployment in the production environment by authorised personnel or system components; 	<p>C5 - 1. Standard Operating Procedures (SOPs), that define the procedures required to operate and maintain the Service environment, have been established and communicated to employees. SOPs are reviewed and approved annually by appropriate management.</p> <p>CM - 1. Procedures for managing different types of changes to the features are documented and communicated.</p> <p>CM - 3. Responsibilities for approving and implementing changes to the features are segregated among designated personnel.</p>	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
<ul style="list-style-type: none"> • Requirements for the performance and documentation of tests; • Requirements for segregation of duties during development, testing and release of changes; • Requirements for the proper information of cloud customers about the type and scope of the change as well as the resulting obligations to cooperate in accordance with the contractual agreements; • Requirements for the documentation of changes in system, operational and user documentation; and • Requirements for the implementation and documentation of emergency changes that must comply with the same level of security as normal changes. 		
<p>DEV-04 The Cloud Service Provider provides a training program for regular, target group-oriented security training and awareness for internal and external employees on standards and methods of secure software development and provision as well as on how to use the tools used for this purpose. The program is regularly reviewed and updated with regard to the applicable policies and instructions, the assigned roles and responsibilities and the tools used.</p>	<p>IS - 4. An information security education and awareness program is established that includes policy training and periodic security updates to Azure DevOps personnel.</p> <p>SDL - 1. Development of new features and changes to existing features follow a defined approach based on the Microsoft Secure Development Lifecycle (SDL) methodology.</p> <p>ELC - 6. Management expects outsourced providers to meet certain levels of skills and experience, depending on the role and holds them accountable to achieving specific deliverables, as outlined in a Statement of Work. Outsourced providers are trained to understand and comply with Microsoft's supplier code of conduct.</p>	<p>No exceptions noted.</p>

C5 Criteria	Azure DevOps Activity	Test Result
<p>DEV-05 In accordance with the applicable policies (cf. DEV-03), changes are subjected to a risk assessment with regard to potential effects on the system components concerned and are categorised and prioritised accordingly.</p>	<p>CM - 1. Procedures for managing different types of changes to the features are documented and communicated.</p> <p>CM - 2. Key stakeholders approve changes prior to release into production based on documented change management procedures.</p>	No exceptions noted.
<p>DEV-06 Changes to the cloud service are subject to appropriate testing during software development and deployment.</p> <p>The type and scope of the tests correspond to the risk assessment. The tests are carried out by appropriately qualified personnel of the Cloud Service Provider or by automated test procedures that comply with the state-of-the-art. Cloud customers are involved into the tests in accordance with the contractual requirements.</p> <p>The severity of the errors and vulnerabilities identified in the tests, which are relevant for the deployment decision, is determined according to defined criteria and actions for timely remediation or mitigation are initiated.</p>	<p>CM - 1. Procedures for managing different types of changes to the features are documented and communicated.</p> <p>CM - 2. Key stakeholders approve changes prior to release into production based on documented change management procedures.</p> <p>CM - 4. Software releases and configuration changes are tested based on established criteria prior to production implementation.</p> <p>CM - 5. Implemented changes are reviewed for adherence to established procedures prior to closure. Changes are rolled back to their previous state in case of errors or security concerns.</p>	No exceptions noted.
<p>DEV-07 System components and tools for source code management and software deployment that are used to make changes to system components of the cloud service in the production environment are subject to a role and rights concept according to IDM-01 and authorisation mechanisms. They must be configured in such a way that all changes</p>	<p>SDL - 5. Azure DevOps services use code repositories for managing source code changes. Procedures are established to authorize access for personnel based on their role and submit changes to source code. Code changes submitted to the code repository are logged and can be traced to the individuals or system components executing them.</p> <p>CM - 2. Key stakeholders approve changes prior to release into production based on documented change management procedures.</p>	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
are logged and can therefore be traced back to the individuals or system components executing them.	CM - 3. Responsibilities for approving and implementing changes to the features are segregated among designated personnel.	
DEV-08 Version control procedures are set up to track dependencies of individual changes and to restore affected system components back to their previous state as a result of errors or identified vulnerabilities.	CM - 5. Implemented changes are reviewed for adherence to established procedures prior to closure. Changes are rolled back to their previous state in case of errors or security concerns.	No exceptions noted.
DEV-09 Authorised personnel or system components of the Cloud Service Provider approve changes to the cloud service based on defined criteria (e.g. test results and required approvals) before these are made available to the cloud customers in the production environment. Cloud customers are involved in the release according to contractual requirements.	CM - 1. Procedures for managing different types of changes to the features are documented and communicated. CM - 2. Key stakeholders approve changes prior to release into production based on documented change management procedures. CM - 5. Implemented changes are reviewed for adherence to established procedures prior to closure. Changes are rolled back to their previous state in case of errors or security concerns.	No exceptions noted.
DEV-10 Production environments are physically or logically separated from test or development environments to prevent unauthorised access to cloud customer data, the spread of malware, or changes to system components. Data contained in the production environments is not used in test or development environments in order not to compromise their confidentiality.	SDL - 4. Separate environments, outside of production, are established for the purpose of developing and testing changes. Production data is not replicated in test or development environments. SDL - 7. Source code builds are scanned for malware prior to release to production.	No exceptions noted.

SSO: Control and Monitoring of Service Providers and Suppliers

Control Objective 5.12: Ensure the protection of information that service providers or suppliers of the Cloud Service Provider (subcontractors) can access and monitor the agreed services and security requirements.

C5 Criteria	Azure DevOps Activity	Test Result
<p>SSO-01 Policies and instructions for controlling and monitoring third parties (e.g. service providers or suppliers) whose services contribute to the provision of the cloud service are documented, communicated and provided in accordance with SP-01 with respect to the following aspects:</p> <ul style="list-style-type: none"> • Requirements for the assessment of risks resulting from the procurement of third-party services; • Requirements for the classification of third parties based on the risk assessment by the Cloud Service Provider and the determination of whether the third party is a subcontractor (cf. Supplementary Information); • Information security requirements for the processing, storage or transmission of information by third parties based on recognised industry standards; • Information security awareness and training requirements for staff; • applicable legal and regulatory requirements; • Requirements for dealing with vulnerabilities, security incidents and malfunctions; 	<p>C5 - 1. Standard Operating Procedures (SOPs), that define the procedures required to operate and maintain the Service environment, have been established and communicated to employees. SOPs are reviewed and approved annually by appropriate management.</p> <p>C5 - 9. Prior to contracting with Microsoft, suppliers undergo a risk assessment based on the services that will be provided and data handled. List of reviewed suppliers is maintained and their risk profiles are reviewed at least annually.</p> <p>SOC2 - 10. Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees must acknowledge Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage.</p> <p>SOC2 - 17. Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within Azure DevOps environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Legal and Corporate Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements.</p> <p>IS - 4. An information security education and awareness program is established that includes policy training and periodic security updates to Azure DevOps personnel.</p> <p>ELC - 6. Management expects outsourced providers to meet certain levels of skills and experience, depending on the role and holds them accountable to achieving specific deliverables, as outlined in a Statement of Work. Outsourced providers are trained to understand and comply with Microsoft's supplier code of conduct.</p>	<p>No exceptions noted.</p>

C5 Criteria	Azure DevOps Activity	Test Result
<ul style="list-style-type: none"> • Specifications for the contractual agreement of these requirements; • Specifications for the monitoring of these requirements; and • Specifications for applying these requirements also to service providers used by the third parties, insofar as the services provided by these service providers also contribute to the provision of the cloud service. 		
<p>SSO-02 Service providers and suppliers of the Cloud Service Provider undergo a risk assessment in accordance with the policies and instructions for the control and monitoring of third parties prior to contributing to the delivery of the cloud service. The adequacy of the risk assessment is reviewed regularly, at least annually, by qualified personnel of the Cloud Service Provider during service usage.</p> <p>The risk assessment includes the identification, analysis, evaluation, handling and documentation of risks with regard to the following aspects:</p> <ul style="list-style-type: none"> • Protection needs regarding the confidentiality, integrity, availability and authenticity of information processed, stored or transmitted by the third party; • Impact of a protection breach on the provision of the cloud service; 	<p>C5 - 1. Standard Operating Procedures (SOPs), that define the procedures required to operate and maintain the Service environment, have been established and communicated to employees. SOPs are reviewed and approved annually by appropriate management.</p> <p>C5 - 9. Prior to contracting with Microsoft, suppliers undergo a risk assessment based on the services that will be provided and data handled. List of reviewed suppliers is maintained and their risk profiles are reviewed at least annually.</p> <p>SOC2 - 17. Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within Azure DevOps environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Legal and Corporate Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements.</p> <p>SOC2 - 18. Microsoft Azure DevOps performs an annual risk assessment that covers security, continuity, and operational risks. As part of this process, threats to security are identified and risks from these threats are formally assessed.</p>	<p>No exceptions noted.</p>

C5 Criteria	Azure DevOps Activity	Test Result
<ul style="list-style-type: none"> • The Cloud Service Provider's dependence on the service provider or supplier for the scope, complexity and uniqueness of the service purchased, including the consideration of possible alternatives. 		
<p>SSO-03 The Cloud Service Provider maintains a directory for controlling and monitoring the service providers and suppliers who contribute services to the delivery of the cloud service. The following information is maintained in the directory:</p> <ul style="list-style-type: none"> • Company name; • Address; • Locations of data processing and storage; • Responsible contact person at the service provider/supplier; • Responsible contact person at the cloud service provider; • Description of the service; • Classification based on the risk assessment; • Beginning of service usage; and • Proof of compliance with contractually agreed requirements. <p>The information in the list is checked at least annually for completeness, accuracy and validity.</p>	<p>SOC2 - 17. Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within Azure DevOps environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Legal and Corporate Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements.</p> <p>C5 - 9. Prior to contracting with Microsoft, suppliers undergo a risk assessment based on the services that will be provided and data handled. List of reviewed suppliers is maintained and their risk profiles are reviewed at least annually.</p>	<p>No exceptions noted.</p>

C5 Criteria	Azure DevOps Activity	Test Result
<p>SSO-04 The Cloud Service Provider monitors compliance with information security requirements and applicable legal and regulatory requirements in accordance with policies and instructions concerning controlling and monitoring of third-parties.</p> <p>Monitoring includes a regular review of the following evidence to the extent that such evidence is to be provided by third parties in accordance with the contractual agreements:</p> <ul style="list-style-type: none"> • reports on the quality of the service provided; • certificates of the management systems' compliance with international standards; • independent third-party reports on the suitability and operating effectiveness of their service-related internal control systems; and • Records of the third parties on the handling of vulnerabilities, security incidents and malfunctions. <p>The frequency of the monitoring corresponds to the classification of the third party based on the risk assessment conducted by the Cloud Service Provider (cf. SSO-02). The results of the monitoring are included in the review of the third party's risk assessment.</p> <p>Identified violations and deviations are subjected to analysis, evaluation and treatment in accordance with the risk management procedure (cf. OIS-07).</p>	<p>C5 - 12. Management has developed and documented a risk assessment policy to address the purpose, scope, roles, responsibilities for managing deviations from the security policies/standards. The risk assessment policy and procedures are reviewed and updated on an annual basis.</p> <p>SOC2 - 15. Microsoft performs annual Information Security Management System (ISMS) review and results are reviewed with management.</p> <p>This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.</p> <p>SOC2 - 17. Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within Azure DevOps environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Legal and Corporate Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements.</p> <p>SOC2 - 18. Microsoft Azure DevOps performs an annual risk assessment that covers security, continuity, and operational risks. As part of this process, threats to security are identified and risks from these threats are formally assessed.</p> <p>SOC2 - 19. Microsoft Azure DevOps undergoes independent audits and assessments, at least annually, to monitor and verify compliance with security requirements. Findings are recorded, reviewed, prioritized, and remediation plans are developed.</p> <p>ELC - 5. Internal Audit Charter directs Internal Audit to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment.</p>	<p>No exceptions noted.</p>

C5 Criteria	Azure DevOps Activity	Test Result
<p>SSO-05 The Cloud Service Provider has defined and documented exit strategies for the purchase of services where the risk assessment of the service providers and suppliers regarding the scope, complexity and uniqueness of the purchased service resulted in a very high dependency (cf. Supplementary Information).</p> <p>Exit strategies are aligned with operational continuity plans and include the following aspects:</p> <ul style="list-style-type: none"> • Analysis of the potential costs, impacts, resources and timing of the transition of a purchased service to an alternative service provider or supplier; • Definition and allocation of roles, responsibilities and sufficient resources to perform the activities for a transition; • Definition of success criteria for the transition; • Definition of indicators for monitoring the performance of services, which should initiate the withdrawal from the service if the results are unacceptable. 	<p>SOC2 - 17. Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within Azure DevOps environment based on Microsoft’s corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Legal and Corporate Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements.</p> <p>SOC2 - 18. Microsoft Azure DevOps performs an annual risk assessment that covers security, continuity, and operational risks. As part of this process, threats to security are identified and risks from these threats are formally assessed.</p> <p>C5 - 9. Prior to contracting with Microsoft, suppliers undergo a risk assessment based on the services that will be provided and data handled. List of reviewed suppliers is maintained and their risk profiles are reviewed at least annually.</p>	<p>No exceptions noted.</p>

SIM: Security Incident Management

Control Objective 5.13: Ensure a consistent and comprehensive approach to the capture, assessment, communication and escalation of security incidents.

C5 Criteria	Azure DevOps Activity	Test Result
<p>SIM-01 Policies and instructions with technical and organisational safeguards are documented, communicated and provided in accordance with SP-01 to ensure a fast, effective and proper response to all known security incidents.</p> <p>The Cloud Service Provider defines guidelines for the classification, prioritisation and escalation of security incidents and creates interfaces to the incident management and business continuity management.</p> <p>In addition, the Cloud Service Provider has set up a "Computer Emergency Response Team" (CERT), which contributes to the coordinated resolution of occurring security incidents.</p> <p>Customers affected by security incidents are informed in a timely and appropriate manner.</p>	<p>C5 - 1. Standard Operating Procedures (SOPs), that define the procedures required to operate and maintain the Service environment, have been established and communicated to employees. SOPs are reviewed and approved annually by appropriate management.</p> <p>IM - 1. An incident management framework is established and communicated with defined processes, roles and responsibilities for the detection, escalation and response of incidents.</p> <p>IM - 3. The Service Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures.</p> <p>SOC2 - 6. The service maintains and notifies customers of potential changes, and security and availability type of events that may impact the service, through an online Service Dashboard. Changes to the security commitments and security obligations of the service's customers are updated on the Azure DevOps website in a timely manner.</p>	No exceptions noted.
<p>SIM-02 Subject matter experts of the Cloud Service Provider, together with external security providers where appropriate, classify, prioritise and perform root-cause analyses for events that could constitute a security incident.</p>	<p>IM - 2. Events, thresholds and metrics are defined and configured to detect incidents and alert the associated Service Operations team.</p> <p>IM - 3. The Service Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures.</p> <p>IM - 4. Incident post-mortem activities are conducted for high severity incidents impacting the service environment.</p>	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
	VM - 8. Penetration testing is performed on critical infrastructure components at least annually. Findings are documented, tracked and remediated.	
<p>SIM-03 After a security incident has been processed, the solution is documented in accordance with the contractual agreements and the report is sent to the affected customers for final acknowledgement or, if applicable, as confirmation.</p>	<p>C5 - 6. Microsoft Azure DevOps has established forensic procedures to support potential legal action after an information security incident.</p> <p>IM - 4. Incident post-mortem activities are conducted for high severity incidents impacting the service environment.</p> <p>SOC2 - 6. The service maintains and notifies customers of potential changes, and security and availability type of events that may impact the service, through an online Service Dashboard. Changes to the security commitments and security obligations of the service's customers are updated on the Azure DevOps website in a timely manner.</p>	No exceptions noted.
<p>SIM-04 The Cloud Service Provider informs employees and external business partners of their obligations. If necessary, they agree to or are contractually obliged to report all security events that become known to them and are directly related to the cloud service provided by the Cloud Service Provider to a previously designated central office of the Cloud Service Provider promptly.</p> <p>In addition, the Cloud Service Provider communicates that "false reports" of events that do not subsequently turn out to be incidents do not have any negative consequences.</p>	<p>IS - 3. Management has established defined roles and responsibilities to oversee implementation of the information security policy across the service.</p> <p>IM - 1. An incident management framework is established and communicated with defined processes, roles and responsibilities for the detection, escalation and response of incidents.</p> <p>SOC2 - 10. Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees must acknowledge Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage.</p> <p>ELC - 6. Management expects outsourced providers to meet certain levels of skills and experience, depending on the role and holds them accountable to achieving specific deliverables, as outlined in a Statement of Work. Outsourced providers are trained to understand and comply with Microsoft's supplier code of conduct.</p>	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
<p>SIM-05 Mechanisms are in place to measure and monitor the type and scope of security incidents and to report them to support agencies. The information obtained from the evaluation is used to identify recurrent or significant incidents and to identify the need for further protection.</p>	<p>IM - 1. An incident management framework is established and communicated with defined processes, roles and responsibilities for the detection, escalation and response of incidents.</p> <p>IM - 2. Events, thresholds and metrics are defined and configured to detect incidents and alert the associated Service Operations team.</p> <p>IM - 3. The Service Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures.</p> <p>IM - 4. Incident post-mortem activities are conducted for high severity incidents impacting the service environment.</p>	<p>No exceptions noted.</p>

BCM: Business Continuity Management

Control Objective 5.14: Plan, implement, maintain and test procedures and measures for business continuity and emergency management.

C5 Criteria	Azure DevOps Activity	Test Result
<p>BCM-01 The top management (or a member of the top management) of the Cloud Service Provider is named as the process owner of business continuity and emergency management and is responsible for establishing the process within the company as well as ensuring compliance with the guidelines. They must ensure that sufficient resources are made available for an effective process.</p> <p>People in management and other relevant leadership positions demonstrate leadership and commitment to this issue by encouraging employees to actively contribute to the effectiveness of continuity and emergency management.</p>	<p>BC - 3. Microsoft has developed a Business Continuity and Disaster Recovery (BC / DR) Standard Operating Procedure and documentation that includes the defined information security and availability requirements.</p>	No exceptions noted.
<p>BCM-02 Policies and instructions to determine the impact of any malfunction to the cloud service or enterprise are documented, communicated and made available in accordance with SP-01. The following aspects are considered as minimum:</p> <ul style="list-style-type: none">• Possible scenarios based on a risk analysis;• Identification of critical products and services	<p>BC - 1. Management conducts a risk assessment to identify and assess continuity risks related to Azure DevOps. The Business Impact Analysis is carried out and impacts are assessed for critical services based on revenue and operations considerations.</p> <p>BC - 2. Business Continuity Plans (BCP) are documented and published for critical services, which provide roles and responsibilities and detailed procedures for recovery and reconstitution of systems to a known state per defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Plans are reviewed on an annual basis, at a minimum.</p> <p>BC - 3. Microsoft has developed a Business Continuity and Disaster Recovery (BC / DR) Standard Operating Procedure and documentation that includes the defined information security and availability requirements.</p>	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
<ul style="list-style-type: none"> • Identify dependencies, including processes (including resources required), applications, business partners and third parties; • Capture threats to critical products and services; • Identification of effects resulting from planned and unplanned malfunctions and changes over time; • Determination of the maximum acceptable duration of malfunctions; • Identification of restoration priorities; • Determination of time targets for the resumption of critical products and services within the maximum acceptable time period (RTO); • Determination of time targets for the maximum reasonable period during which data can be lost and not recovered (RPO); and • Estimation of the resources needed for resumption. 		
<p>BCM-03 Based on the business impact analysis, a single framework for operational continuity and business plan planning will be implemented, documented and enforced to ensure that all plans are consistent. Planning is based on established standards, which are documented in a "Statement of Applicability".</p>	<p>BC - 2. Business Continuity Plans (BCP) are documented and published for critical services, which provide roles and responsibilities and detailed procedures for recovery and reconstitution of systems to a known state per defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Plans are reviewed on an annual basis, at a minimum.</p> <p>BC - 4. The BCP team conducts testing of the business continuity and disaster recovery plans at least annually. Issues identified during testing are resolved during the exercises and plans are updated accordingly.</p>	<p>No exceptions noted.</p>

C5 Criteria	Azure DevOps Activity	Test Result
<p>Business continuity plans and contingency plans take the following aspects into account:</p> <ul style="list-style-type: none"> • Defined purpose and scope with consideration of the relevant dependencies; • Accessibility and comprehensibility of the plans for persons who are to act accordingly; • Ownership by at least one designated person responsible for review, updating and approval; • Defined communication channels, roles and responsibilities including notification of the customer; • Recovery procedures, manual interim solutions and reference information (taking into account prioritisation in the recovery of cloud infrastructure components and services and alignment with customers); • Methods for putting the plans into effect; • Continuous process improvement; and • Interfaces to Security Incident Management. 		
<p>BCM-04. The business impact analysis, business continuity plans and contingency plans are reviewed, updated and tested on a regular basis (at least annually) or after significant organisational or environmental changes. Tests involve affected customers (tenants) and relevant third parties. The tests are documented and results are taken</p>	<p>BC - 2. Business Continuity Plans (BCP) are documented and published for critical services, which provide roles and responsibilities and detailed procedures for recovery and reconstitution of systems to a known state per defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Plans are reviewed on an annual basis, at a minimum.</p>	<p>No exceptions noted.</p>

C5 Criteria	Azure DevOps Activity	Test Result
into account for future operational continuity measures.	BC - 4. The BCP team conducts testing of the business continuity and disaster recovery plans at least annually. Issues identified during testing are resolved during the exercises and plans are updated accordingly.	

COM: Compliance

Control Objective 5.15: Avoid non-compliance with legal, regulatory, self-imposed or contractual information security and compliance requirements.

C5 Criteria	Azure DevOps Activity	Test Result
COM-01 The legal, regulatory, self-imposed and contractual requirements relevant to the information security of the cloud service as well as the Cloud Service Provider's procedures for complying with these requirements are explicitly defined and documented.	<p>SOC2 - 13. Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization.</p> <p>SOC2 - 14. Microsoft manages a compliance program with representation from various cross-functional teams including CELA, Marketing, security champions to identify and manage compliance with relevant statutory, regulatory and contractual requirements.</p>	No exceptions noted.
<p>COM-02 Policies and instructions for planning and conducting audits are documented, communicated and made available in accordance with SP-01 and address the following aspects:</p> <ul style="list-style-type: none"> • Restriction to read-only access to system components in accordance with the agreed audit plan and as necessary to perform the activities; 	<p>SOC2 - 15. Microsoft performs annual Information Security Management System (ISMS) review and results are reviewed with management.</p> <p>This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.</p> <p>SOC2 - 19. Microsoft Azure DevOps undergoes independent audits and assessments, at least annually, to monitor and verify compliance with security requirements. Findings are recorded, reviewed, prioritized, and remediation plans are developed.</p>	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
<ul style="list-style-type: none"> • Activities that may result in malfunctions to the cloud service or breaches of contractual requirements are performed during scheduled maintenance windows or outside peak periods; and • Logging and monitoring of activities. 		
<p>COM-03 Subject matter experts check the compliance of the information security management system at regular intervals, at least annually, with the relevant and applicable legal, regulatory, self-imposed or contractual requirements (cf. COM-01) as well as compliance with the policies and instructions (cf. SP-01) within their scope of responsibility (cf. OIS-01) through internal audits</p> <p>Identified vulnerabilities and deviations are subject to risk assessment in accordance with the risk management procedure (cf. OIS-06) and follow-up measures are defined and tracked (cf. OPS-18).</p>	<p>SOC2 - 13. Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization.</p> <p>SOC2 - 15. Microsoft performs annual Information Security Management System (ISMS) review and results are reviewed with management.</p> <p>This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.</p> <p>SOC2 - 18. Microsoft Azure DevOps performs an annual risk assessment that covers security, continuity, and operational risks. As part of this process, threats to security are identified and risks from these threats are formally assessed.</p> <p>SOC2 - 19. Microsoft Azure DevOps undergoes independent audits and assessments, at least annually, to monitor and verify compliance with security requirements. Findings are recorded, reviewed, prioritized, and remediation plans are developed.</p>	No exceptions noted.
<p>COM-04 The top management of the Cloud Service Provider is regularly informed about the information security performance within the scope of the ISMS in order to ensure its continued suitability, adequacy and effectiveness. The information is included in the management review of the ISMS at is performed at least once a year.</p>	<p>IS - 3. Management has established defined roles and responsibilities to oversee implementation of the information security policy across the service.</p> <p>PI - 2. Azure DevOps management reviews portal performance periodically to evaluate compliance with customer SLA requirements.</p> <p>SOC2 - 15. Microsoft performs annual Information Security Management System (ISMS) review and results are reviewed with management.</p>	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
	<p>This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.</p> <p>SOC2 - 18. Microsoft Azure DevOps performs an annual risk assessment that covers security, continuity, and operational risks. As part of this process, threats to security are identified and risks from these threats are formally assessed.</p>	

INQ: Dealing with investigation requests from government agencies

Control Objective 5.16: Ensure appropriate handling of government investigation requests for legal review, information to cloud customers, and limitation of access to or disclosure of data.

C5 Criteria	Azure DevOps Activity	Test Result
INQ-01 Investigation requests from government agencies are subjected to a legal assessment by subject matter experts of the Cloud Service Provider. The assessment determines whether the government agency has an applicable and legally valid legal basis and what further steps need to be taken.	C5 - 8. Procedures to evaluate government investigative demands for customer data are established and documented. Procedures include a review and assessment by the Microsoft legal department, which will evaluate the legal basis for the request to determine what response is required, notify the impacted customer where permitted by law, where Microsoft is required to produce customer data, work with engineering to collect and produce the minimum data responsive to the request as required by law. Procedures are reviewed at least annually.	No exceptions noted.
INQ-02 The Cloud Service Provider informs the affected Cloud Customer(s) without undue delay, unless the applicable legal basis on which the government agency is based prohibits this or there are clear indications of illegal actions in connection with the use of the Cloud Service.	C5 - 8. Procedures to evaluate government investigative demands for customer data are established and documented. Procedures include a review and assessment by the Microsoft legal department, which will evaluate the legal basis for the request to determine what response is required, notify the impacted customer where permitted by law, where Microsoft is required to produce customer data, work with engineering to collect and produce the minimum data responsive to the request as required by law. Procedures are reviewed at least annually.	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
<p>INQ-03 Access to or disclosure of cloud customer data in connection with government investigation requests is subject to the provision that the Cloud Service Provider's legal assessment has shown that an applicable and valid legal basis exists and that the investigation request must be granted on that basis.</p>	<p>C5 - 8. Procedures to evaluate government investigative demands for customer data are established and documented. Procedures include a review and assessment by the Microsoft legal department, which will evaluate the legal basis for the request to determine what response is required, notify the impacted customer where permitted by law, where Microsoft is required to produce customer data, work with engineering to collect and produce the minimum data responsive to the request as required by law. Procedures are reviewed at least annually.</p>	<p>No exceptions noted.</p>
<p>INQ-04 The Cloud Service Provider's procedures establishing access to or disclosing data of cloud customers in the context of investigation requests from governmental agencies ensure that the agencies only gain access to or insight into the data that is the subject of the investigation request.</p> <p>If no clear limitation of the data is possible, the Cloud Service Provider anonymises or pseudonymises the data so that government agencies can only assign it to those cloud customers who are subject of the investigation request.</p>	<p>C5 - 8. Procedures to evaluate government investigative demands for customer data are established and documented. Procedures include a review and assessment by the Microsoft legal department, which will evaluate the legal basis for the request to determine what response is required, notify the impacted customer where permitted by law, where Microsoft is required to produce customer data, work with engineering to collect and produce the minimum data responsive to the request as required by law. Procedures are reviewed at least annually.</p>	<p>No exceptions noted.</p>

PSS: Product Safety and Security

Control Objective 5.17: Provides up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorisation of users of cloud customers.

C5 Criteria	Azure DevOps Activity	Test Result
<p>PSS-01 The Cloud Service Provider provides cloud customers with guidelines and recommendations for the secure use of the cloud service provided. The information contained therein is intended to assist the cloud customer in the secure configuration, installation and use of the cloud service, to the extent applicable to the cloud service and the responsibility of the cloud user.</p> <p>The type and scope of the information provided will be based on the needs of subject matter experts of the cloud customers who set information security requirements, implement them or verify the implementation (e.g. IT, Compliance, Internal Audit). The information in the guidelines and recommendations for the secure use of the cloud service address the following aspects, where applicable to the cloud service:</p> <ul style="list-style-type: none">• Instructions for secure configuration;• Information sources on known vulnerabilities and update mechanisms;• Error handling and logging mechanisms;• Authentication mechanisms;	<p>SOC2 - 4. The service maintains and communicates the confidentiality and related security obligations for customer data via the Microsoft Trust Center. Guidelines and recommendations for the secure use of the cloud services, as applicable, are communicated to customers.</p> <p>SOC2 - 5. The service maintains and distributes an accurate system description to authorized users.</p> <p>SOC2 - 7. Prior to engaging in service, customers are required to review and agree with the acceptable use of data and the Service, as well as security and privacy requirements, which are defined in the Microsoft Online Services Use Rights, Microsoft Online Subscription Agreement, Privacy Statement and Technical Overview of the Security Features.</p> <p>C5 - 7. Azure DevOps has published a standard set of APIs with an ecosystem of tools and libraries on the Azure DevOps Portal.</p>	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
<ul style="list-style-type: none"> • Roles and rights concept including combinations that result in an elevated risk; and • Services and functions for administration of the cloud service by privileged users. <p>The information is maintained so that it is applicable to the cloud service provided in the version intended for productive use.</p>		
<p>PSS-02 The Cloud Service Provider applies appropriate measures to check the cloud service for vulnerabilities which might have been integrated into the cloud service during the software development process.</p> <p>The procedures for identifying such vulnerabilities are part of the software development process and, depending on a risk assessment, include the following activities:</p> <ul style="list-style-type: none"> • Static Application Security Testing; • Dynamic Application Security Testing; • Code reviews by the Cloud Service Provider's subject matter experts; and • Obtaining information about confirmed vulnerabilities in software libraries provided by third parties and used in their own cloud service. <p>The severity of identified vulnerabilities is assessed according to defined criteria and measures are taken to immediately eliminate or mitigate them.</p>	<p>CM - 5. Implemented changes are reviewed for adherence to established procedures prior to closure. Changes are rolled back to their previous state in case of errors or security concerns.</p> <p>SDL - 1. Development of new features and changes to existing features follow a defined approach based on the Microsoft Secure Development Lifecycle (SDL) methodology.</p> <p>SDL - 2. Applicable operational security and internal control requirements are documented and approved for Azure DevOps.</p> <p>SDL - 6. A security review of releases is performed on a periodic basis by designated security personnel within Azure DevOps.</p> <p>SDL - 7. Source code builds are scanned for malware prior to release to production.</p> <p>VM - 5. Procedures are established to evaluate and implement Microsoft released patches to service components.</p> <p>VM - 6. Procedures are established to monitor production and supporting infrastructure for known security vulnerabilities. Identified security vulnerabilities are remediated.</p> <p>VM - 8. Penetration testing is performed on critical infrastructure components at least annually. Findings are documented, tracked and remediated.</p> <p>SOC2 - 12. The security baselines are refreshed for Azure DevOps on a periodic basis.</p>	<p>No exceptions noted.</p>

C5 Criteria	Azure DevOps Activity	Test Result
<p>PSS-03 The Cloud Service Provider operates or refers to a daily updated online register of known vulnerabilities that affect the Cloud Service Provider and assets provided by the Cloud Service Provider that the cloud customers have to install, provide or operate themselves under the customers responsibility.</p> <p>The presentation of the vulnerabilities follows the Common Vulnerability Scoring System (CVSS).</p> <p>The online register is easily accessible to any cloud customer. The information contained therein forms a suitable basis for risk assessment and possible follow-up measures on the part of cloud users.</p> <p>For each vulnerability, it is indicated whether software updates (e.g. patch, update) are available, when they will be rolled out and whether they will be deployed by the Cloud Service Provider, the cloud customer or both of them together.</p>	<p>VM - 5. Procedures are established to evaluate and implement Microsoft released patches to service components.</p> <p>VM - 6. Procedures are established to monitor production and supporting infrastructure for known security vulnerabilities. Identified security vulnerabilities are remediated.</p> <p>SOC2 - 6. The service maintains and notifies customers of potential changes, and security and availability type of events that may impact the service, through an online Service Dashboard. Changes to the security commitments and security obligations of the service's customers are updated on the Azure DevOps website in a timely manner.</p> <p>SOC2 - 12. The security baselines are refreshed for Azure DevOps on a periodic basis.</p>	<p>No exceptions noted.</p>
<p>PSS-04 The cloud service provided is equipped with error handling and logging mechanisms. These enable cloud users to obtain security-related information about the security status of the cloud service as well as the data, services or functions it provides.</p> <p>The information is detailed enough to allow cloud users to check the following aspects,</p>	<p>VM - 1. Production and supporting infrastructure are configured to log and collect security events.</p> <p>VM - 2. Administrator activity is logged.</p> <p>VM - 3. A monitoring system is implemented on production and supporting infrastructure to monitor the service for potential malicious activity and intrusion past service trust boundaries.</p> <p>VM - 9. Azure DevOps provides logging mechanisms that can be configured by customers to log activities and metrics.</p>	<p>No exceptions noted.</p>

C5 Criteria	Azure DevOps Activity	Test Result
<p>insofar as they are applicable to the cloud service:</p> <ul style="list-style-type: none"> • Which data, services or functions available to the cloud user within the cloud service, have been accessed by whom and when (Audit Logs); • Malfunctions during processing of automatic or manual actions; and • Changes to security-relevant configuration parameters, error handling and logging mechanisms, user authentication, action authorisation, cryptography, and communication security. <p>The logged information is protected from unauthorised access and modification and can be deleted by the Cloud Customer.</p> <p>If the cloud customer is responsible for the activation or type and scope of logging, the Cloud Service Provider must provide appropriate logging capabilities.</p>	<p>LA - 1. External access to customer data stored in the service requires authentication.</p> <p>LA - 5. Customer-configured authorization settings can be set to further restrict authentication methods.</p> <p>SOC2 - 6. The service maintains and notifies customers of potential changes, and security and availability type of events that may impact the service, through an online Service Dashboard. Changes to the security commitments and security obligations of the service's customers are updated on the Azure DevOps website in a timely manner.</p> <p>C5 - 2. Availability of logging and monitoring software is monitored by internal tools on a continuous basis, and responsible personnel is notified in case of any failure.</p> <p>C5 - 4. Customer metadata is collected, retained, and removed based on the documented procedures.</p> <p>C5 - 5. Logging servers are required to authenticate over encrypted channel to access logs generated within the production environment. Access to logging and monitoring infrastructure is restricted to authorized personnel.</p>	
<p>PSS-05 The Cloud Service Provider provides authentication mechanisms that can force strong authentication (e.g. two or more factors) for users, IT components or applications within the cloud users' area of responsibility.</p> <p>These authentication mechanisms are set up at all access points that allow users, IT components or applications to interact with the cloud service.</p>	<p>LA - 1. External access to customer data stored in the service requires authentication.</p> <p>LA - 2. Customer credentials used to access the service meet the applicable password policy requirements.</p> <p>LA - 5. Customer-configured authorization settings can be set to further restrict authentication methods.</p> <p>OA - 4. Password complexity standards are defined and enforced for Azure DevOps personnel credentials.</p>	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
For privileged users, IT components or applications, these authentication mechanisms are enforced.	OA - 10. Access to production resources requires the use of a Secure Admin Workstation (SAW) which requires MFA for access. SAWs are hardened and secured devices with restricted access.	
PSS-06 To protect confidentiality, availability, integrity and authenticity during interactions with the cloud service, a suitable session management system is used that at least corresponds to the state-of-the-art and is protected against known attacks. Mechanisms are implemented that invalidate a session after it has been detected as inactive. The inactivity can be detected by time measurement. In this case, the time interval can be configured by the Cloud Service Provider or - if technically possible - by the cloud customer.	LA - 6. User sessions within the service portal expire after a stipulated period of inactivity.	No exceptions noted.
PSS-07 If passwords are used as authentication information for the cloud service, their confidentiality is ensured by the following procedures: <ul style="list-style-type: none"> • Users can initially create the password themselves or must change an initial password when logging in to the cloud service for the first time. An initial password loses its validity after a maximum of 14 days. • When creating passwords, compliance with the length and complexity requirements of the Cloud Service Provider (cf. IDM-09) or the cloud customer is technically enforced. 	LA - 2. Customer credentials used to access the service meet the applicable password policy requirements.	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
<ul style="list-style-type: none"> • The user is informed about changing or resetting the password. • The server-side storage takes place using state-of-the-art cryptographically strong hash functions in combination with at least 32-bit long salt values. 		
<p>PSS-08 The Cloud Service Provider provides cloud users with a roles and rights concept for managing access rights. It describes rights profiles for the functions provided by the cloud service.</p> <p>The rights profiles are suitable for enabling cloud users to manage access authorisations and permissions in accordance with the principle of least-privilege and how it is necessary for the performance of tasks ("need-to-know principle") and to implement the principle of functional separation between operational and controlling functions ("separation of duties").</p>	<p>C5 - 1. Standard Operating Procedures (SOPs), that define the procedures required to operate and maintain the Service environment, have been established and communicated to employees. SOPs are reviewed and approved annually by appropriate management.</p> <p>OA - 1. Administrative access to the service is controlled through defined interfaces that require authentication using AD credentials.</p> <p>OA - 2. Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning access to employees, contractors, and service providers to specific applications or information resources.</p> <p>SDL - 3. Responsibilities for production deployment are segregated within the feature teams.</p> <p>CM - 3. Responsibilities for approving and implementing changes to the features are segregated among designated personnel.</p>	No exceptions noted.
<p>PSS-09 Access to the functions provided by the cloud service is restricted by access controls (authorisation mechanisms) that verify whether users, IT components, or applications are authorised to perform certain actions.</p> <p>The Cloud Service Provider validates the functionality of the authorisation mechanisms before new functions are made available to cloud users and in the event of changes to the authorisation mechanisms of</p>	<p>OA - 1. Administrative access to the service is controlled through defined interfaces that require authentication using AD credentials.</p> <p>OA - 2. Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning access to employees, contractors, and service providers to specific applications or information resources.</p> <p>OA - 6. Procedures are established for granting temporary access for personnel to customer data and applications upon appropriate approval.</p> <p>CM - 4. Software releases and configuration changes are tested based on established criteria prior to production implementation.</p>	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
existing functions (cf. DEV-06). The severity of identified vulnerabilities is assessed according to defined criteria based on industry standard metrics (e.g. Common Vulnerability Scoring System) and measures for timely resolution or mitigation are initiated. Vulnerabilities that have not been fixed are listed in the online register of known vulnerabilities (cf. PSS-02).	<p>VM - 5. Procedures are established to evaluate and implement Microsoft released patches to service components.</p> <p>VM - 6. Procedures are established to monitor production and supporting infrastructure for known security vulnerabilities. Identified security vulnerabilities are remediated.</p>	
<p>PSS-10 If the Cloud Service offers functions for software-defined networking (SDN), the confidentiality of the data of the cloud user is ensured by suitable SDN procedures.</p> <p>The Cloud Service Provider validates the functionality of the SDN functions before providing new SDN features to cloud users or modifying existing SDN features. Identified defects are assessed and corrected in a risk-oriented manner.</p>	This C5 criteria is not applicable as Azure DevOps is SaaS offering only.	No exceptions noted.
<p>PSS-11 If cloud customers operate virtual machines or containers with the cloud service, the Cloud Service Provider must ensure the following aspects:</p> <ul style="list-style-type: none"> • The cloud customer can restrict the selection of images of virtual machines or containers according to his specifications, so that users of this cloud customer can only launch the images or containers released according to these restrictions. • If the Cloud Service Provider provides images of virtual machines or containers to 	This C5 criteria is not applicable as Azure DevOps is SaaS offering only.	No exceptions noted.

C5 Criteria	Azure DevOps Activity	Test Result
<p>the Cloud Customer, the Cloud Service Provider appropriately inform the Cloud Customer of the changes made to the previous version.</p> <ul style="list-style-type: none"> • In addition, these images provided by the Cloud Service Provider are hardened according to generally accepted industry standards. 		
<p>PSS-12 The cloud customer is able to specify the locations (location/country) of the data processing and storage including data backups according to the contractually available options.</p> <p>This must be ensured by the cloud architecture.</p>	<p>DS - 7. Customer data is automatically replicated to minimize isolated faults. Customers are able to determine geographical regions of the data processing and storage, including data backups.</p>	<p>No exceptions noted.</p>

Part C: Azure DevOps Control Activities and Test Results

Control Title	Control Activity	Test Procedures	Results of Tests
IS - 1	Microsoft has documented and communicated a security policy that defines the information security rules and requirements for the Azure DevOps environment.	<ul style="list-style-type: none">Inquired of the management if a documented security policy that specifies the rules and requirements applicable to the Azure DevOps environment exists.Obtained and inspected the security policy to ascertain that it addresses the applicable information security requirements.Inspected the security policy to ascertain that it was published and communicated to Azure DevOps' employees and the relevant third parties.	No exceptions noted.
IS - 2	The security policy is reviewed and approved annually by Microsoft management.	<ul style="list-style-type: none">Inquired of the management to gain an understanding of the process for reviewing and approving the security policy.Obtained and inspected evidence of the annual security policy review performed and the associated management approvals to ascertain that it was reviewed annually.	No exceptions noted.
IS - 3	Management has established defined roles and responsibilities to oversee implementation of the information security policy across the service.	<ul style="list-style-type: none">Inquired of the management to gain an understanding of the implementation of the security policy requirements within Azure DevOps through the designation of roles and responsibilities.Inspected relevant documentation (e.g., SOPs) to ascertain that roles and responsibilities for implementation of security policy requirements were defined and documented.	No exceptions noted.
IS - 4	An information security education and awareness program is established that includes policy training and periodic security updates to Azure DevOps personnel.	<ul style="list-style-type: none">Inquired of the management to gain an understanding of the processes for awareness and training on information security for employees, contractors, and third-party users.Inspected training material to ascertain that it incorporated policy training and periodic security updates.	No exceptions noted.

Control Title	Control Activity	Test Procedures	Results of Tests
		<ul style="list-style-type: none"> Obtained participation details for mandatory security trainings and ascertained that participation was tracked for Azure DevOps personnel. 	
OA - 1	Administrative access to the service is controlled through defined interfaces that require authentication using AD credentials.	<ul style="list-style-type: none"> Inquired of the management to gain an understanding of the procedures in place for accessing Azure DevOps-specific administration tools. For a sample of administration tools, obtained and inspected evidence to ascertain that access to the administration tools was restricted through defined interfaces, authenticated through AD credentials, and was limited based on the job responsibilities. Obtained and inspected the current listing of user accounts and ascertained that each user was assigned a unique user ID which clearly identifies the user. 	No exceptions noted.
OA - 2	Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning access to employees, contractors, and service providers to specific applications or information resources.	<ul style="list-style-type: none"> Inquired of the management regarding the approvals required from the security group owners for accessing specific applications or information resources. Observed the use of account management tools to ascertain if access was granted to users only upon receipt of approval from Full-Time Employee (FTE) managers or their delegates. 	No exceptions noted.
OA - 3	Procedures are in place to disable accounts on a timely basis, upon the user's termination.	<ul style="list-style-type: none"> Inquired of the Operations team that procedures are established for disabling terminated user accounts in a timely manner. For all terminated users within the examination period, obtained account disablement logs to ascertain that accounts were disabled timely upon termination. 	No exceptions noted.
OA - 4	Password complexity standards are defined and enforced for	<ul style="list-style-type: none"> Inquired of the management to gain an understanding of the implementation of password standards (e.g., length, complexity and age) and acceptable use guidelines. 	No exceptions noted.

Control Title	Control Activity	Test Procedures	Results of Tests
	Azure DevOps personnel credentials.	<ul style="list-style-type: none"> Obtained the relevant configuration files to ascertain that password standards were enforced. 	
OA - 5	Access privileges are reviewed quarterly to determine if access rights are commensurate to the user's job duties. Access is modified based on the results of the reviews.	<ul style="list-style-type: none"> Inquired of the management to gain an understanding of the process in place and the cadence for periodic user access reviews. Obtained review documentation for sampled quarters to ascertain whether access reviews were performed per the defined cadence and resulting action items were completed by the owners / delegates of the feature. 	No exceptions noted.
OA - 6	Procedures are established for granting temporary access for personnel to customer data and applications upon appropriate approval.	<ul style="list-style-type: none"> Inquired of management to understand the procedures in place for granting and revoking temporary access to internal administration services. For a sample of services, obtained and inspected temporary access logs and associated tickets to ascertain that temporary access was granted and approved per the defined process and had documented business justification associated with it. 	No exceptions noted.
OA - 7	Authentication over an encrypted Remote Desktop Connection is used for administrator access to the production environment.	<ul style="list-style-type: none"> Inquired of the management to understand mechanisms in place for connecting remotely to the Azure DevOps environment. Observed access sessions to ascertain that Remote Desktop Protocol (RDP) connections to the Azure DevOps environment were authenticated and encrypted. 	No exceptions noted.
OA - 8	Alerts are generated when a break-glass account is used to access production environment.	<ul style="list-style-type: none"> Inquired of the management to understand the procedures in place for monitoring break-glass account access to the production environment. Obtained and inspected the configuration files to ascertain that automated mechanisms were in place to generate alerts when a break-glass account is used to access the production environment. 	No exceptions noted.

Control Title	Control Activity	Test Procedures	Results of Tests
OA - 9	Production domain-level user accounts are disabled after a stipulated period of inactivity.	<ul style="list-style-type: none"> Inquired of the management team if procedures for disabling user accounts that have been inactive after a stipulated period in the production environment are established. Obtained and inspected the applicable configuration settings to ascertain that production domain accounts were disabled timely after their inactivity period. 	No exceptions noted.
OA - 10	Access to production resources requires the use of a Secure Admin Workstation (SAW) which requires MFA for access. SAWs are hardened and secured devices with restricted access.	<ul style="list-style-type: none"> Inquired of the management to understand the process of using Secure Admin Workstation (SAW) machine and authentication using MFA for accessing production resources. Observed the access and authentication mechanisms to ascertain that access to production resources required using Secure Admin Workstation (SAW) machine and MFA for authentication. Obtained and inspected the configuration settings for SAW devices and ascertained that the devices are hardened and have restricted access. 	No exceptions noted.
DS - 1	Cryptographic certificates, keys, and customer access keys used for communication between the features and other internal components are stored securely and are rotated on a periodic basis.	<ul style="list-style-type: none"> Inquired of the management to understand the different types of cryptographic certificates and keys used by the service to connect to internal components, and their cadence / frequency of rotation. Inspected the location of the cryptographic keys, customer access keys, connection strings and Storage Account Keys (SAKs) to ascertain that they were encrypted. Additionally, inspected security groups having access to secrets to ascertain that access was strictly restricted to personnel having valid business justification. Obtained the list of production secrets and for a sample of production secrets, obtained the last rotated date to ascertain that the secrets were rotated on a periodic basis. 	No exceptions noted.
DS - 2	Customer data communicated through service interfaces is	<ul style="list-style-type: none"> Inquired of the management regarding controls in place that restrict transmission of customer data using secure protocols through various endpoints over external networks. 	No exceptions noted.

Control Title	Control Activity	Test Procedures	Results of Tests
	encrypted during transmission over external networks.	<ul style="list-style-type: none"> Reperformed the control to ascertain that the restrictions were in place to prevent use of insecure protocols for transmission of customer data over external networks. 	
DS - 3	Internal communication between key components where customer data is transmitted / involved is secured using SSL or equivalent mechanism(s).	<ul style="list-style-type: none"> Inquired of the management to understand the use of secure mechanisms such as Secure Sockets Layer (SSL) with mutual authentication for communication between internal key components that involves customer data. For a sample of Azure DevOps components, performed inspection to ascertain the use of Secure Sockets Layer (SSL) for internal communication. 	No exceptions noted.
DS - 4	Cryptographic controls are used for information protection within the platform based on the Cryptographic Policy and Key Management procedures.	<ul style="list-style-type: none"> Inquired of the management regarding the policies and procedures in place for using cryptographic controls within the Azure DevOps environment. Inspected a sample of releases to ascertain that Cryptographic Policy and Key Management requirements were enforced. 	No exceptions noted.
DS - 5	Backups of key service components are performed regularly and stored in fault tolerant (isolated) facilities. Backups are monitored and backup errors are investigated and followed-up on appropriately.	<ul style="list-style-type: none"> Inquired of the management regarding the procedures in place for backing up the Azure DevOps service components. For a sample of components, obtained and inspected configurations and logs to ascertain that component data was backed up and stored in fault tolerant (isolated) facilities. Obtained and inspected the configuration used to create incident tickets to ascertain that backup errors were investigated and remediated appropriately. 	No exceptions noted.
DS - 6	Critical Azure DevOps components are designed with redundancy to sustain isolated	<ul style="list-style-type: none"> Inquired of the management regarding the redundancy mechanisms in place for key components within the Azure DevOps platform. 	No exceptions noted.

Control Title	Control Activity	Test Procedures	Results of Tests
	faults and minimize disruptions to customer services.	<ul style="list-style-type: none"> For a sample of critical Azure DevOps components, performed inspection to ascertain that redundancies were implemented within the production environment to minimize the disruptions to customer services. 	
DS - 7	Customer data is automatically replicated to minimize isolated faults. Customers are able to determine geographical regions of the data processing and storage, including data backups.	<ul style="list-style-type: none"> Inquired of the management regarding the redundancy mechanisms in place to replicate customer data stored across Azure DevOps features. For a sample of Azure DevOps features, observed configuration and replication status to ascertain that customer data was automatically replicated to minimize isolated faults. Observed the customer portal and available options to ascertain that the customers are able to determine geographical regions of the data processing and storage, including data backups. 	No exceptions noted.
DS - 8	Upon termination of a customer account, the customer data is removed based upon the stipulated retention and removal timelines.	<ul style="list-style-type: none"> Inquired of the management regarding the policy and procedures in place for the retention and removal of customer data upon deletion of Azure DevOps account. For a sample of terminated customer accounts, inspected logged database events to ascertain that data was retained or removed as per the stipulated retention and removal timelines noted in the Azure DevOps data retention and removal policies. 	No exceptions noted.
CM - 1	Procedures for managing different types of changes to the features are documented and communicated.	<ul style="list-style-type: none"> Inquired of the management regarding the procedures for managing various types of changes to the Azure DevOps environment including requirements for tracking, approval and testing. Obtained and inspected the Change Management procedure documentation to ascertain that procedures for requesting, classifying, approving, and implementing changes were defined and communicated. 	No exceptions noted.
CM - 2	Key stakeholders approve changes prior to release into production based on	<ul style="list-style-type: none"> Inquired of the management about the procedures for approving changes prior to release into production. 	No exceptions noted.

Control Title	Control Activity	Test Procedures	Results of Tests
	documented change management procedures.	<ul style="list-style-type: none"> For a sample of changes implemented to production, obtained and inspected evidence to ascertain that changes were approved by key stakeholders and executed in accordance with documented procedures. 	
CM - 3	Responsibilities for approving and implementing changes to the features are segregated among designated personnel.	<ul style="list-style-type: none"> Inquired of the management about the procedures for segregation of duties for key responsibilities related to change implementation and approval. Obtained and inspected policy documentation and ascertained that segregation of duties for key responsibilities was documented. For a sample of branch policy setting, inspected the branch policy configuration to ascertain that responsibilities for approving and implementing changes to the features are segregated among designated personnel. For a sample of changes implemented to production, obtained and inspected evidence to ascertain that approval and implementation of changes were segregated among designated personnel. 	No exceptions noted.
CM - 4	Software releases and configuration changes are tested based on established criteria prior to production implementation.	<ul style="list-style-type: none"> Inquired of the management regarding the procedures for testing various types of changes to the Azure DevOps environment. For a sample of changes made to production, obtained and inspected evidence to ascertain that documented procedures for testing were followed prior to deployment. 	No exceptions noted.
CM - 5	Implemented changes are reviewed for adherence to established procedures prior to closure. Changes are rolled back to their previous state in case of errors or security concerns.	<ul style="list-style-type: none"> Inquired of the management regarding the procedures for reviewing various types of changes to the Azure DevOps environment prior to closure. For a sample of changes made to production, obtained and inspected evidence to ascertain that changes were reviewed prior to closure. Further, ascertained that changes were rolled back to their previous state if errors or security issue identified during review. 	No exceptions noted.

Control Title	Control Activity	Test Procedures	Results of Tests
CM - 6	Any changes to production via break-glass have been reviewed to ensure all changes were appropriate.	<ul style="list-style-type: none"> Inquired of the management to gain an understanding of the process related to performing review of changes made through break-glass accounts in the production environment. For a sample of break-glass account access scenarios, obtained and inspected tickets to ascertain that change was reviewed for appropriateness. 	No exceptions noted.
SDL - 1	Development of new features and changes to existing features follow a defined approach based on the Microsoft Secure Development Lifecycle (SDL) methodology.	<ul style="list-style-type: none"> Inquired of the management to gain an understanding of the SDL methodology followed for the development of new features and making changes to existing features. For a sample of releases, inspected SDL documentation to ascertain that SDL methodology was followed to incorporate security practices as part of the development process. For a sample of changes, obtained and inspected evidence to ascertain that documented procedures for testing were followed prior to deployment. 	No exceptions noted.
SDL - 2	Applicable operational security and internal control requirements are documented and approved for Azure DevOps.	<ul style="list-style-type: none"> Inquired of the management regarding the process to identify and document applicable security and internal control requirements as part of the SDL process. For a sample of releases, inspected documentation to ascertain that security and internal control requirements were identified, documented, and approved based on review with designated security leads. 	No exceptions noted.
SDL - 3	Responsibilities for production deployment are segregated within the feature teams.	<ul style="list-style-type: none"> Inquired of the management to understand the processes in place to segregate responsibilities for production deployment within the feature teams. Obtained and inspected evidence for a sample of production deployments to ascertain that access to perform production deployments was restricted to authorized Azure DevOps teams. 	No exceptions noted.

Control Title	Control Activity	Test Procedures	Results of Tests
SDL - 4	Separate environments, outside of production, are established for the purpose of developing and testing changes. Production data is not replicated in test or development environments.	<ul style="list-style-type: none"> Inquired of the management around separation of development, test, and production environments. Obtained and inspected configuration files to ascertain that the development, test and production environments existed and were separate. Obtained and inspected database configuration files to ascertain that production data is not replicated to the test or development environments. 	No exceptions noted.
SDL - 5	Azure DevOps services use code repositories for managing source code changes. Procedures are established to authorize access for personnel based on their role and submit changes to source code. Code changes submitted to the code repository are logged and can be traced to the individuals or system components executing them.	<ul style="list-style-type: none"> Inquired of the management regarding the access control procedures for source code. Inspected user access within the code repository tool to ascertain that access was restricted to authorized users based on their role. For a sample source code repository, observed the configuration files and a change to ascertain that the identity of the individual and / or system component changing the code, the time of the change, and changes submitted to the source code repository were logged. 	No exceptions noted.
SDL - 6	A security review of releases is performed on a periodic basis by designated security personnel within Azure DevOps.	<ul style="list-style-type: none"> Inquired of the management to gain an understanding of the procedures for security review of releases. For a sample of releases, inspected documentation to ascertain that a security review was completed as per the SDL methodology and sign-offs were obtained from the designated security personnel. 	No exceptions noted.
SDL - 7	Source code builds are scanned for malware prior to release to production.	<ul style="list-style-type: none"> Inquired of the management regarding the procedures in place to scan source code builds for malware. 	No exceptions noted.

Control Title	Control Activity	Test Procedures	Results of Tests
		<ul style="list-style-type: none"> For a sample of source code builds, obtained and inspected evidence of scan build for malwares to ascertain that malware scanning was performed automatically as part of the build process prior to release to production. 	
VM - 1	Production and supporting infrastructure are configured to log and collect security events.	<ul style="list-style-type: none"> Inquired of the management that security event logging is configured for key components within Azure DevOps platform components and supporting infrastructure to enable detection of security events. For a sample of platform components and supporting infrastructure, obtained and inspected configurations to ascertain that logging of security events was enabled. Also, obtained and inspected an automated alert and associated monitoring. 	No exceptions noted.
VM - 2	Administrator activity is logged.	<ul style="list-style-type: none"> Inquired of the management regarding the mechanisms in place for logging administrator activities within Azure DevOps platform. For a sample of platform components and supporting infrastructure, obtained and inspected configurations to ascertain that logging of administrator activities was enabled. Also, obtained and inspected an automated alert, associated monitoring and corresponding log of administrator activity. 	No exceptions noted.
VM - 3	A monitoring system is implemented on production and supporting infrastructure to monitor the service for potential malicious activity and intrusion past service trust boundaries.	<ul style="list-style-type: none"> Inquired of the management regarding the monitoring capabilities within the Azure DevOps environment to detect potential malicious activity and intrusions. For a sample of platform components and supporting infrastructure, obtained and inspected configurations to ascertain that a monitoring system was in place to detect malicious activities and intrusion. Also, obtained and inspected an automated alert, associated monitoring and corresponding event log. 	No exceptions noted.

Control Title	Control Activity	Test Procedures	Results of Tests
VM - 4	Procedures have been established to investigate and respond to the malicious events detected by the monitoring system for timely resolution.	<ul style="list-style-type: none"> Inquired of the management if incidents and malicious events are detected, investigated, and resolved in a timely manner per documented procedures. Obtained and inspected a sample of incident tickets pertaining to Azure DevOps to ascertain that incidents and malicious events were detected, investigated, and resolved in a timely manner. 	No exceptions noted.
VM - 5	Procedures are established to evaluate and implement Microsoft released patches to service components.	<ul style="list-style-type: none"> Inquired of the management to gain an understanding of the patch management process implemented within the Azure DevOps environment. For a sample of servers, obtained and inspected upgrade configurations or patch installation logs to ascertain whether patches were implemented per documented procedures. 	No exceptions noted.
VM - 6	Procedures are established to monitor production and supporting infrastructure for known security vulnerabilities. Identified security vulnerabilities are remediated.	<ul style="list-style-type: none"> Inquired of the management regarding the procedures in place to monitor the Azure DevOps components and supporting infrastructure for known security vulnerabilities. For a sample of platform components and supporting infrastructure, obtained and inspected configurations to ascertain that monitoring for known security vulnerabilities was enabled. Further, ascertained that identified security vulnerabilities were monitored for remediation. 	No exceptions noted.
VM - 7	The availability of the service is monitored through third-party and internal tools, and the status is communicated through a Service Dashboard.	<ul style="list-style-type: none"> Inquired of the management regarding the procedures and tools for monitoring of service availability. Inspected service dashboards and monitoring tools to ascertain that availability was monitored and status was communicated. 	No exceptions noted.
VM - 8	Penetration testing is performed on critical infrastructure components at least annually. Findings are	<ul style="list-style-type: none"> Inquired of the management about penetration testing performed on the Azure DevOps environment. Obtained and inspected the documents related to penetration testing performed on the Azure DevOps environment to ascertain: 	No exceptions noted.

Control Title	Control Activity	Test Procedures	Results of Tests
	documented, tracked and remediated.	<ul style="list-style-type: none"> Penetration testing was performed at least annually Critical infrastructure components were included in the scope boundary Findings were documented, tracked and remediated based on severity 	
VM - 9	Azure DevOps provides logging mechanisms that can be configured by customers to log activities and metrics.	<ul style="list-style-type: none"> Inquired of the management to understand the logging mechanisms available to customers, and how these logging mechanisms can be leveraged. Reperformed the control to ascertain that logging mechanisms can be configured by customers to log activities and track metrics. Inspected the logs available on the portal and ascertained that expected entries are being logged. 	No exceptions noted.
IM - 1	An incident management framework is established and communicated with defined processes, roles and responsibilities for the detection, escalation and response of incidents.	<ul style="list-style-type: none"> Inquired of the management that information security incidents are managed through designated responsibilities and documented procedures. Obtained information security incident management policy documents to ascertain that roles and responsibilities for detection, escalation and notification to specialist groups during a security incident were established and communicated. 	No exceptions noted.
IM - 2	Events, thresholds and metrics are defined and configured to detect incidents and alert the associated Service Operations team.	<ul style="list-style-type: none"> Inquired of the management about the events, thresholds and metrics established to detect and facilitate alerts / notifications to incident management teams. For a sample of platform components, inspected logs and notifications and ascertained that automated notifications were received upon occurrence of the configured events, thresholds and metrics. 	No exceptions noted.
IM - 3	The Service Operations team performs monitoring, including documentation, classification, escalation, and coordination of	<ul style="list-style-type: none"> Inquired of the management about the procedures in place for 24x7 monitoring and handling of incidents. 	No exceptions noted.

Control Title	Control Activity	Test Procedures	Results of Tests
	incidents per documented procedures.	<ul style="list-style-type: none"> Identified the population of incidents (all severities) within the examination period and obtained and inspected a sample of incident tickets to ascertain that each incident was handled per documented procedures. Obtained and inspected monitoring team schedule to ascertain that monitoring was performed 24x7. 	
IM - 4	Incident post-mortem activities are conducted for high severity incidents impacting the service environment.	<ul style="list-style-type: none"> Inquired of the management about the procedures in place for performing incident post-mortem and submitting formal management reports, for customer impacting, high severity incidents. Inspected a sample of incidents to ascertain whether the service environment was impacted and for those that impacted the service environment, that a post-mortem was performed and relevant sign-off(s) were obtained as per documented procedures. 	No exceptions noted.
LA - 1	External access to customer data stored in the service requires authentication.	<ul style="list-style-type: none"> Inquired of the management to understand the authentication methods in place to restrict external access to customer data stored in Azure DevOps. Reperformed the control to ascertain that authentication was required to access the data stored in the service. 	No exceptions noted.
LA - 2	Customer credentials used to access the service meet the applicable password policy requirements.	<ul style="list-style-type: none"> Inquired of the management to understand the password policies established and enforced for customer credentials. Reperformed the controls to ascertain effective enforcement of password policies. 	No exceptions noted.
LA - 3	Logical segregation is implemented to restrict unauthorized access to other customer tenants.	<ul style="list-style-type: none"> Inquired of the management to understand the controls implemented to enforce logical segregation between customer accounts. Reperformed the control to ascertain that segregation was enforced between accounts, and customers can access data within the service only upon authorization checks. 	No exceptions noted.

Control Title	Control Activity	Test Procedures	Results of Tests
LA - 4	Customer data that is confidential is protected while in storage within the service.	<ul style="list-style-type: none"> Inquired of the management to understand the mechanisms implemented to protect customer confidential data. Inspected mechanisms to ascertain that customer confidential data was protected while in storage. 	No exceptions noted.
LA - 5	Customer-configured authorization settings can be set to further restrict authentication methods.	<ul style="list-style-type: none"> Inquired of the management to understand various authorization settings that the customer can configure. Reperformed the control to ascertain that access was restricted based on customer configured authorization settings. 	No exceptions noted.
LA - 6	User sessions within the service portal expire after a stipulated period of inactivity.	<ul style="list-style-type: none"> Inquired of the management to understand the mechanisms implemented to enforce session timeout on Azure DevOps portal. Inspected the session expiry settings in the Azure DevOps portal and reperformed the control to ascertain that sessions were configured to expire after a stipulated period of inactivity. 	No exceptions noted.
BC - 1	Management conducts a risk assessment to identify and assess continuity risks related to Azure DevOps. The Business Impact Analysis is carried out and impacts are assessed for critical services based on revenue and operations considerations.	<ul style="list-style-type: none"> Inquired of the Business Continuity group to understand the processes in place for evaluating and analyzing risk associated with critical business processes as part of the Business Impact Analysis (BIA). Obtained and inspected the BIA document to ascertain that BIA was completed and impacts were assessed for critical processes / services based on revenue and operations considerations. 	No exceptions noted.
BC - 2	Business Continuity Plans (BCP) are documented and published for critical services, which provide roles and responsibilities and detailed procedures for recovery and	<ul style="list-style-type: none"> Inquired of the Business Continuity group to understand the processes in place for developing and maintaining Business Continuity Plans (BCP). Obtained and inspected the BCP and BIA documents to ascertain that roles and responsibilities and, RTOs / RPOs for critical processes were defined and approved. 	No exceptions noted.

Control Title	Control Activity	Test Procedures	Results of Tests
	reconstitution of systems to a known state per defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Plans are reviewed on an annual basis, at a minimum.	<ul style="list-style-type: none"> Inspected the BCP document to ascertain that it is reviewed and published on an annual basis, at a minimum. 	
BC - 3	Microsoft has developed a Business Continuity and Disaster Recovery (BC / DR) Standard Operating Procedure and documentation that includes the defined information security and availability requirements.	<ul style="list-style-type: none"> Inquired of the Business Continuity group to understand the processes in place for developing and maintaining Business Continuity procedures in alignment with the Microsoft Enterprise Business Continuity Methodology (EBCM) framework. Obtained and inspected the Business Continuity and Disaster Recovery Standard Operating Procedures and Business Continuity plan to ascertain that they included the defined information security and availability requirements. 	No exceptions noted.
BC - 4	The BCP team conducts testing of the business continuity and disaster recovery plans at least annually. Issues identified during testing are resolved during the exercises and plans are updated accordingly.	<ul style="list-style-type: none"> Inquired of the Business Continuity group to understand the procedures in place for testing the Business Continuity and Disaster Recovery plans. For different failover procedures, obtained and inspected the BC / DR testing plan and results documents, including follow-up documentation for issues identified and ascertained that they were established, reviewed and tested at least annually. 	No exceptions noted.
BC - 5	Management has established monitoring mechanisms to address capacity issues in a timely manner.	<ul style="list-style-type: none"> Inquired of the management to understand the procedures established to monitor capacity requirements. Obtained and inspected capacity report for the sampled months to ascertain that management has established monitoring mechanisms to address capacity issues in a timely manner. 	No exceptions noted.

Control Title	Control Activity	Test Procedures	Results of Tests
SOC2 - 1	Service assets are classified in accordance with Microsoft Online Services Classification Guidelines. Microsoft has conducted security categorization for its information and information systems and the results are documented, reviewed and approved by the authorizing official.	<ul style="list-style-type: none"> Inquired of the management to understand the procedures for identification and classification of service assets and data. Obtained and inspected the current asset classification document to ascertain that it addressed the key information and information systems used by Azure DevOps and, reviewed and approved by the authorizing official. Additionally, compared the asset classification to the Standard Operating Procedures (SOP) to ascertain that it aligned with the approved definition criteria in the SOP. 	No exceptions noted.
SOC2 - 2	The service maintains an inventory of key information assets. Procedures are established to review usage of key information assets on at least an annual basis.	<ul style="list-style-type: none"> Inquired of the management to understand the process for reviewing and updating the inventory of key information assets. Obtained and inspected asset usage review report to ascertain that the key information asset inventory was reviewed on at least an annual basis. 	No exceptions noted.
SOC2 - 3	The service maintains a customer support website that describes the process for customers and other external users to inform about potential security issues and submitting complaints. Reported issues are reviewed and addressed per documented incident management procedures.	<ul style="list-style-type: none"> Inquired of the management regarding the customer support website and the process for addressing reported Customer Support Requests. Observed the customer support website and ascertained that it allowed customers to report security issues or complaints. Identified the population of customer support requests within the examination period and obtained tickets for a sample of customer support requests to ascertain that each incident was handled per documented procedures. 	No exceptions noted.
SOC2 - 4	The service maintains and communicates the confidentiality and related security obligations for	<ul style="list-style-type: none"> Inquired of the management to understand the process for maintaining and communicating confidentiality and related security obligations for 	No exceptions noted.

Control Title	Control Activity	Test Procedures	Results of Tests
	customer data via the Microsoft Trust Center. Guidelines and recommendations for the secure use of the cloud services, as applicable, are communicated to customers.	<p>customer data, and recommendations for the secure use of cloud services to customers.</p> <ul style="list-style-type: none"> Inspected the Microsoft Trust Center website to ascertain that confidentiality and security obligations were maintained and communicated to customers and observed that it included security related information and best practices for use of cloud services. Inspected the Microsoft Trust Center website to ascertain that changes to the confidentiality and security obligations were communicated to customers. 	
SOC2 - 5	The service maintains and distributes an accurate system description to authorized users.	<ul style="list-style-type: none"> Inquired of the management to understand the procedures for the development, maintenance, and distribution of the system description. Obtained the Azure DevOps service description to ascertain whether it described the system. Observed if the service description was published and communicated to authorized users. 	No exceptions noted.
SOC2 - 6	The service maintains and notifies customers of potential changes, and security and availability type of events that may impact the service, through an online Service Dashboard. Changes to the security commitments and security obligations of the service's customers are updated on the Azure DevOps website in a timely manner.	<ul style="list-style-type: none"> Inquired of the management to understand the process for notifying customers of security and availability events through the Service Dashboard. Additionally, gained an understanding of the process for updating customers of changes to commitments in a timely manner. Observed and inspected the customer Service Dashboard to ascertain that it was updated with changes and, security and availability type of events that impacted the service. Obtained and inspected a sample customer impacting incident from the incident population, to ascertain that the incident was reflected in the Service Dashboard's history, as applicable. Observed the security commitments and obligations on the Azure DevOps website to ascertain that changes were updated on the Azure DevOps website in a timely manner. 	No exceptions noted.

Control Title	Control Activity	Test Procedures	Results of Tests
SOC2 - 7	Prior to engaging in service, customers are required to review and agree with the acceptable use of data and the Service, as well as security and privacy requirements, which are defined in the Microsoft Online Services Use Rights, Microsoft Online Subscription Agreement, Privacy Statement and Technical Overview of the Security Features.	<ul style="list-style-type: none"> Inquired of the management to understand the procedures for the identification of security requirements and how customers must meet these requirements prior to gaining access to Azure DevOps. Obtained and inspected the End User Licensing Agreement (EULA) or Customer Agreements required by customers to sign / agree to prior to gaining access, and ascertained that they addressed identified security requirements. Reperformed procedures of creating sample account to ascertain that agreements were required to be signed prior to subscription creation. 	No exceptions noted.
SOC2 - 8	Microsoft has defined disciplinary actions for employees and contingent staff that commit a security breach or violate the security policy.	<ul style="list-style-type: none"> Inquired of the HR team regarding: <ul style="list-style-type: none"> Disciplinary actions established for employees and contingent staff who commit a security breach or violate the security policy The process to communicate the policy to employees and relevant external parties Obtained and inspected the HR policy to ascertain that disciplinary actions were included for employees and contingent staff who commit a security breach or violate the security policy. 	No exceptions noted.
SOC2 - 9	Microsoft personnel and contingent staff undergo formal screening, including background verification checks as a part of the hiring process prior to being granted access. Additional screening is conducted in accordance with customer specific requirements,	<ul style="list-style-type: none"> Inquired of the HR team to understand the procedures established to perform background checks on new or transferred personnel before they are granted access to the production assets. Obtained the list of new hires and transfers during the examination period. For a sample of new hires and transfers, obtained and inspected evidence to ascertain that background checks were performed as per the policy prior to employment. 	No exceptions noted.

Control Title	Control Activity	Test Procedures	Results of Tests
	for employees with access to applicable data.		
SOC2 - 10	Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees must acknowledge Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage.	<ul style="list-style-type: none"> Inquired of the HR team if Non-Disclosure Agreements (NDAs) are signed as a part of the onboarding process. Inspected a sample NDA to ascertain that the agreement included requirements for asset protection, and asset return upon termination of employment. For a sample of new hires and transfers, obtained and inspected evidence to ascertain that the NDA form was signed, which includes acknowledgment of the Employee Handbook. Obtained and inspected the employee handbook to ascertain that policies around reporting of misconduct and events were documented. 	No exceptions noted.
SOC2 - 12	The security baselines are refreshed for Azure DevOps on a periodic basis.	<ul style="list-style-type: none"> Inquired of the management regarding the baseline process for Azure DevOps, including scanning environments for baseline compatibility. For a sample of platform components, obtained and inspected configurations to ascertain that logging of baseline deviations was enabled. 	No exceptions noted.
SOC2 - 13	Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization.	<ul style="list-style-type: none"> Inquired of the management to understand the procedures in place for identifying relevant statutory, regulatory, and contractual requirements, and making the relevant updates to documentation or procedures accordingly. Obtained and inspected evidence to ascertain that meetings between Azure DevOps Compliance and Corporate, External, and Legal Affairs (CELA) occur on a periodic basis to define, document and maintain statutory, regulatory, and contractual requirements for Azure DevOps. 	No exceptions noted.

Control Title	Control Activity	Test Procedures	Results of Tests
		<ul style="list-style-type: none"> Obtained and inspected policy, procedure, and agreement documents to ascertain that they were current and included relevant and current statutory, regulatory, and contractual requirements. 	
SOC2 - 14	<p>Microsoft manages a compliance program with representation from various cross-functional teams including CELA, Marketing, security champions to identify and manage compliance with relevant statutory, regulatory and contractual requirements.</p>	<ul style="list-style-type: none"> Inquired of the management to understand the process in place for managing compliance with relevant statutory, regulatory and contractual requirements, with the involvement of various cross-functional teams including CELA, Marketing, and security champions. Inspected evidence to ascertain that the meetings between Azure DevOps Compliance and CELA occurs on a periodic basis. Observed CELA communications regarding regulatory compliance or changes in the regulatory environment. 	No exceptions noted.
SOC2 - 15	<p>Microsoft performs annual Information Security Management System (ISMS) review and results are reviewed with management.</p> <p>This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.</p>	<ul style="list-style-type: none"> Inquired of the management to understand the process in place for performing the Information Security Management System (ISMS) review on an at least annual basis. Obtained and inspected a sample of meeting invites and minutes to ascertain that ISMS review was performed on an ongoing basis through review of scope, security issues, audit results, and monitoring status, and the involvement of management in the entire process. 	No exceptions noted.
SOC2 - 17	<p>Security risks related to external parties (such as customers, contractors and vendors) are identified and</p>	<ul style="list-style-type: none"> Inquired of the management to understand the risk assessment process and how risks are identified and addressed related to external parties (such as customers, contractors and vendors). 	No exceptions noted.

Control Title	Control Activity	Test Procedures	Results of Tests
	addressed within Azure DevOps environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Legal and Corporate Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements.	<ul style="list-style-type: none"> Obtained and inspected the latest risk assessment performed by Azure DevOps management to ascertain that it was completed. Obtained and inspected the Statement of Work (SOW) citing external parties' access was restricted authoritatively based on the risk assessment performed. 	
SOC2 - 18	Microsoft Azure DevOps performs an annual risk assessment that covers security, continuity, and operational risks. As part of this process, threats to security are identified and risks from these threats are formally assessed.	<ul style="list-style-type: none"> Inquired of the management on the annual risk assessment process and how security, continuity and operational risks are addressed. Obtained the risk management framework to ascertain that procedures for identifying, assessing and monitoring risks were established. Obtained and inspected the risk assessment reports for the latest risk assessment performed by Microsoft Azure DevOps management for the identified risk domains, to ascertain that threats to security were identified and the risk from these threats was assessed. 	No exceptions noted.
SOC2 - 19	Microsoft Azure DevOps undergoes independent audits and assessments, at least annually, to monitor and verify compliance with security requirements. Findings are recorded, reviewed, prioritized, and remediation plans are developed.	<ul style="list-style-type: none"> Inquired of the management to understand the independent audit and assessment of compliance with security requirements process and how findings are recorded, reviewed, prioritized, and remediation plans are developed. Obtained and inspected the latest independent audit reports over compliance with security requirements to ascertain that findings were recorded, reviewed, prioritized, and remediation plans were developed. 	No exceptions noted.

Control Title	Control Activity	Test Procedures	Results of Tests
PI - 1	Azure DevOps monitors the transactions invoked by the customer and relays them appropriately to the designated end-point. Actions are taken in response to defined threshold events.	<ul style="list-style-type: none"> Inquired of the management regarding measures in place to monitor transactions invoked by customers. Observed the dashboard used by Azure DevOps for monitoring transactions to ascertain that dashboard provides details regarding transaction processing for the feature teams to review. Obtained evidence to ascertain that repeated transaction processing errors were identified and were tracked for remediation by Azure DevOps feature teams. 	No exceptions noted.
PI - 2	Azure DevOps management reviews portal performance periodically to evaluate compliance with customer SLA requirements.	<ul style="list-style-type: none"> Inquired of the management regarding the review procedures that are established to understand and evaluate portal performance against customer SLA requirements. Obtained and inspected sample weekly Live Site Review (LSR) reports to ascertain that performance reviews were conducted as per established procedures. Obtained and inspected the scheduled meeting invites with leadership to ascertain that performance reviews were conducted as per established procedures. 	No exceptions noted.
PI - 3	Azure DevOps performs input validation to restrict any non-permissible requests to the API.	<ul style="list-style-type: none"> Inquired of the management to understand mechanisms to perform input validation to restrict non-permissible requests. Reperformed the control to ascertain that invalid input provided by the user was detected and error messages were generated. 	No exceptions noted.
PI - 4	Azure DevOps appropriately provisions the services based on request from customer through the portal/API.	<ul style="list-style-type: none"> Inquired of the management to understand mechanisms to provision services to the users through the portal/API based on the customer request. Reperformed the control to ascertain that services were provisioned based on the input parameters provided by the customer. 	No exceptions noted.

Control Title	Control Activity	Test Procedures	Results of Tests
C5 - 1	Standard Operating Procedures (SOPs), that define the procedures required to operate and maintain the Service environment, have been established and communicated to employees. SOPs are reviewed and approved annually by appropriate management.	<ul style="list-style-type: none"> Inquired of the management regarding the process for establishing, maintaining, updating and reviewing Standard Operating Procedures. Obtained and inspected the latest Standard Operating Procedures (SOPs) to ascertain they included appropriate attributes, and were reviewed and approved in a timely manner. 	No exceptions noted.
C5 - 2	Availability of logging and monitoring software is monitored by internal tools on a continuous basis, and responsible personnel is notified in case of any failure.	<ul style="list-style-type: none"> Inquired of the management to understand the procedures in place for monitoring availability of the logging and monitoring infrastructure. Inspected monitoring tool configuration to ascertain that automated mechanisms were in place to continuously identify unavailability of the logging and monitoring infrastructure, and route incidents to appropriate personnel for resolution. 	No exceptions noted.
C5 - 3	Microsoft Azure DevOps components are configured to use Coordinated Universal Time (UTC) time and the clocks are synchronized with the domain controller server.	<ul style="list-style-type: none"> Inquired of the management to ascertain the procedures in place for time synchronization across the various Azure DevOps components. Additionally, inquired if Azure DevOps uses a centralized synchronized time-service protocol (such as Network Time Protocol (NTP)), which synchronizes with UTC, to ascertain that systems, including domain controllers have a common time reference. Observed mechanisms used by Azure DevOps to ascertain that there are configurations in place to sync time and clocks across the Azure DevOps components, including domain controllers, to UTC. 	No exceptions noted.
C5 - 4	Customer metadata is collected, retained, and removed based on the documented procedures.	<ul style="list-style-type: none"> Inquired of the management to understand the process regarding customer metadata collection, retention and deletion. For a sampled user account obtained metadata collected and inspected configurations to ascertain that mechanisms existed for collecting, 	No exceptions noted.

Control Title	Control Activity	Test Procedures	Results of Tests
		retaining and deleting customer metadata in accordance with documented procedures.	
C5 - 5	Logging servers are required to authenticate over encrypted channel to access logs generated within the production environment. Access to logging and monitoring infrastructure is restricted to authorized personnel.	<ul style="list-style-type: none"> Inquired of the management to understand the process and mechanism in place for enforcing authenticated access to the logging and monitoring infrastructure. Through observation and inspection of security configurations, ascertained that mechanisms existed for logging servers to establish an authenticated connection with the logging infrastructure and that it takes place over an encrypted channel. Through inspection ascertained that only authorized individuals were part of the security group that had access to logging and monitoring infrastructure. 	No exceptions noted.
C5 - 6	Microsoft Azure DevOps has established forensic procedures to support potential legal action after an information security incident.	<ul style="list-style-type: none"> Inquired of the management regarding the forensic procedures in place for preservation and presentation of evidence, to support potential legal action after an information security incident. Obtained and inspected forensic procedures and ascertained that procedures and methodologies for gathering and securing evidences were defined. 	No exceptions noted.
C5 - 7	Azure DevOps has published a standard set of APIs with an ecosystem of tools and libraries on the Azure DevOps Portal.	<ul style="list-style-type: none"> Inquired of the management regarding the list of Application Programming Interfaces (APIs) that Azure DevOps offers to customers. Inspected the Azure DevOps API reference webpage to ascertain that the list of APIs offered by Azure DevOps to customers were published in a centralized repository (webpage) and were as per the industry standards. 	No exceptions noted.
C5 - 8	Procedures to evaluate government investigative demands for customer data are established and documented. Procedures include a review	<ul style="list-style-type: none"> Inquired of the management to understand the procedures established to evaluate, review, notify and respond to government investigative demands for customer data. 	No exceptions noted.

Control Title	Control Activity	Test Procedures	Results of Tests
	and assessment by the Microsoft legal department, which will evaluate the legal basis for the request to determine what response is required, notify the impacted customer where permitted by law, where Microsoft is required to produce customer data, work with engineering to collect and produce the minimum data responsive to the request as required by law. Procedures are reviewed at least annually.	<ul style="list-style-type: none"> Obtained and inspected the procedures established for government investigative demands for customer data and ascertained that they were reviewed on an annual basis. 	
C5 - 9	Prior to contracting with Microsoft, suppliers undergo a risk assessment based on the services that will be provided and data handled. List of reviewed suppliers is maintained and their risk profiles are reviewed at least annually.	<ul style="list-style-type: none"> Inquired of the management to gain an understanding of risk assessment performed prior to contracting with suppliers and the process for maintaining the directory of suppliers including their risk profile. Obtained and inspected the directory of suppliers to ascertain that it contained basic supplier information including their risk profile. Additionally, obtained and inspected documented procedures related to performing risk assessment of suppliers to ascertain that the assessment was based on the services provided and data handled. For a sample of suppliers, obtained and inspected the risk assessment report to ascertain that the supplier's risk profile aligned with the services provided and data handled by the suppliers. Additionally, ascertained that the risk profiles were reviewed at least on an annual basis. 	No exceptions noted.
C5 - 10	Microsoft has established policies for mobile computing devices to meet appropriate security practices prior to being connected to the production environment.	<ul style="list-style-type: none"> Inquired of the management that a documented policy exists that specifies the rules and requirements applicable to mobile computing devices. Obtained and inspected the mobile computing policy to ascertain that it included applicable information security requirements. 	No exceptions noted.

Control Title	Control Activity	Test Procedures	Results of Tests
C5 - 11	Azure DevOps has implemented tools to perform integrity verification checks to detect unauthorized changes to software, firmware and information.	<ul style="list-style-type: none"> Inquired of the management regarding the tools implemented to detect unauthorized changes to software, firmware and information. For a sample of platform components and supporting infrastructure, obtained and inspected configurations to ascertain that logging of integrity verification checks was enabled. 	No exceptions noted.
C5 - 12	Management has developed and documented a risk assessment policy to address the purpose, scope, roles, responsibilities for managing deviations from the security policies/standards. The risk assessment policy and procedures are reviewed and updated on an annual basis.	<ul style="list-style-type: none"> Inquired of the management regarding the procedures to manage and review deviations from the security policies/standards. Obtained and inspected the exception procedures, describing the process followed for handling deviations and exceptions. Obtained and inspected the review history for the exception policy to ascertain that it is reviewed at least annually. 	No exceptions noted.
C5 - 13	Customer data is accessible within agreed upon services in data formats compatible with providing those services.	<ul style="list-style-type: none"> Inquired of the management regarding the accessibility of data from agreed upon services in data formats compatible with the services. Reperformed the control to ascertain that customer data was accessible in the data formats compatible with providing those services. 	No exceptions noted.
ELC - 1	Microsoft's values are accessible to employees via the Values SharePoint site and are updated as necessary by management.	<ul style="list-style-type: none"> Inquired of the management regarding Microsoft's values and the process for updating and making them accessible to employees. Observed the Values SharePoint site and ascertained that Microsoft's values are defined, updated as needed, and published to employees. 	No exceptions noted.
ELC - 2	Microsoft Compliance and Ethics team updates the Standards of Business Conduct (SBC) as necessary and the Code is made available	<ul style="list-style-type: none"> Inquired of the Microsoft Compliance and Ethics team to ascertain that Standards of Business Conduct (SBC) is established and made available internally and externally. 	No exceptions noted.

Control Title	Control Activity	Test Procedures	Results of Tests
	internally and externally. The SBC reflects Microsoft's continued commitment to ethical business practices and regulatory compliance. Compliance and Ethics team provides an annual Standards of Business Conduct training course that is mandatory for all employees. Employees who do not complete the training on time are tracked and followed up with appropriately.	<ul style="list-style-type: none"> Obtained and inspected the Standards of Business Conduct to ascertain that the Code included Microsoft's continued commitment to ethical business practices and regulatory compliance. For a sample of employees, obtained the SBC training completion status, including, where applicable, any follow-up documentation for employees who did not complete the training on time. 	
ELC - 3	Microsoft maintains several mechanisms (email, phone, fax, website) that permit employees and non-employees to communicate confidential and / or anonymous reports concerning Business Conduct.	<ul style="list-style-type: none"> Inquired of Microsoft Compliance and Ethics team regarding the mechanisms (email, phone, fax, website) that permit reporting of issues related to Business Conduct. Accessed each communication mechanism to ascertain that the mechanisms were available and functioning. 	No exceptions noted.
ELC - 4	The Audit Committee (AC) reviews its Charter and Responsibilities as listed in its calendar on an annual basis. The AC Responsibilities include meeting with the external and internal auditors on a quarterly basis; providing oversight on the development and performance of controls; and completing an annual self-evaluation.	<ul style="list-style-type: none"> Inquired of the members of the Audit Committee (AC) to gain an understanding of the Charter and Responsibilities of the Audit Committee and its annual review process. Obtained and inspected the agenda or meeting minutes to ascertain the annual review of Audit Committee's Charter and Responsibilities Calendar. Inspected the investor relations website to ascertain that the Audit Committee's Charter and Responsibilities Calendar was published on the website. Obtained evidence (e.g., meeting invite, meeting minutes) to ascertain quarterly meetings between AC and internal / external auditors. 	No exceptions noted.

Control Title	Control Activity	Test Procedures	Results of Tests
ELC - 5	Internal Audit Charter directs Internal Audit to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment.	<ul style="list-style-type: none"> Inquired of the management to gain an understanding of the Internal Audit Charter and the scope and frequency of assurance activities performed by Internal Audit. Obtained and inspected the Internal Audit Charter and ascertained that the Charter directed the services of the Internal Audit. Obtained and inspected the Internal Audit plan and ascertained that the assurance activities were based on an annual risk assessment. 	No exceptions noted.
ELC - 6	Management expects outsourced providers to meet certain levels of skills and experience, depending on the role and holds them accountable to achieving specific deliverables, as outlined in a Statement of Work. Outsourced providers are trained to understand and comply with Microsoft's supplier code of conduct.	<ul style="list-style-type: none"> Inquired of the management regarding the process for: <ul style="list-style-type: none"> Citing expectations from outsourced providers to achieve specific deliverables Training outsourced providers on Microsoft's supplier code of conduct Obtained and inspected Microsoft's SOW template to ascertain that it cited outsourced providers' role and accountability in achieving specific deliverables. Inspected the supplier procurement website to ascertain that Microsoft's supplier code of conduct is available and accessible to all outsourced providers. Observed during the supplier access provisioning process that completion of the supplier code of conduct training is required. 	No exceptions noted.
ELC - 7	Employees hold periodic connects with their managers to validate they are on the expected career path and facilitate greater collaboration. Employees also review their performance against their documented deliverables	<ul style="list-style-type: none"> Inquired of the Human Resources (HR) team that periodic connects take place at least annually, where employee's commitments are evaluated by his or her manager. Obtained and inspected the documentation of a sample periodic connect to ascertain that it included an evaluation of the employee's performance against the documented deliverables (priorities). 	No exceptions noted.

Control Title	Control Activity	Test Procedures	Results of Tests
	(priorities) and discuss the results with their managers.	<ul style="list-style-type: none"> For a sample of employees, obtained evidence of occurrence of periodic connects to ascertain that the connects occurred at least annually. 	
ELC - 8	The Compensation Committee is responsible for reviewing and discussing plans for executive officer development and corporate succession plans for the CEO and other executive officers.	<ul style="list-style-type: none"> Inquired of the members of the Compensation Committee to gain an understanding of the process for planning of executive officer development and corporate succession plans for the CEO and other executive officers. Obtained and inspected the agenda or meeting minutes to ascertain the annual discussion of the succession plans. Inspected the Compensation Committee Charter on the investor relations website to ascertain that the Compensation Committee's responsibility included reviewing the succession plan for CEO and other executive officers, on an annual basis. 	No exceptions noted.
ELC - 9	The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management.	<ul style="list-style-type: none"> Inquired of the Enterprise Risk Management (ERM) team on the ERM risk assessment process and how risks are identified and managed. Obtained and inspected the agenda or meeting minutes to ascertain that the ERM risk assessment results are reviewed bi-annually and presented to the Board of Directors for review and consideration of the changes. 	No exceptions noted.

Section V: Other Information Provided by Management of Microsoft

Section V: Other Information Provided by Management of Microsoft

The information included in Section V of this report is presented by Microsoft to provide additional information to user entities and is not part of Microsoft's description of the system. The information included here in Section V has not been subjected to the procedures applied in the examination of the description of the system related to description of the system, and, accordingly, Deloitte & Touche LLP expresses no opinion on it.

User Entity Responsibilities

The following list includes user entity responsibilities that Microsoft assumes its user entities have implemented, but are not required to meet the relevant applicable trust services criteria:

- Customers are responsible for reporting to Azure DevOps the incidents and alerts that are specific to their Azure DevOps accounts.
- Customers utilizing Azure Active Directory (AAD) services are responsible for implementing appropriate authentication mechanisms and limiting administrative access to appropriate individuals to maintain integrity of their Azure DevOps account.
- Customers are responsible for establishing appropriate controls over the use of their Microsoft Accounts and passwords.
- Customers are responsible for reviewing the access activities associated with their Azure DevOps accounts.
- Customers are responsible for appropriate protection of the secrets associated with their accounts.
- Customers' administrators are responsible for the selection and use of their passwords.
- Customers are responsible for ensuring that authorized users are added to their accounts.
- Customers are responsible to implement logical access controls to provide reasonable assurance that unauthorized access to Azure DevOps projects is restricted.
- Customers are responsible to assign unique IDs and secure passwords to users and customers accessing their Azure DevOps account.
- Customers are responsible for ensuring the supervision, management and control of access to data stored on Azure DevOps.
- Customers are responsible for managing compliance with applicable laws / regulations.
- Customers are responsible for following appropriate security practices while using Azure DevOps features.
- Customers are responsible for maintaining their own system(s) of record.
- Customers are responsible for backup of their data from Azure DevOps to local storage upon Azure DevOps account termination.
- Customers are responsible for backup of data prior to account deletion.
- Customers are responsible for specifying authorization requirements for their internet-facing messaging end-points.
- Customers are responsible for following a Secure Development Lifecycle for their applications developed using Azure DevOps.