Microsoft

NOTE: You may not distribute this SOC 2 report for Microsoft Azure to other parties, except where Microsoft Azure is a component of the services you deliver to your customers. In this circumstance, you may distribute this SOC 2 report to current and prospective customers / users of your own services. You must provide recipients of this SOC 2 report written documentation of the function that Microsoft provides as it relates to your services. You must keep a complete and accurate record of entities and the personnel of such entities to whom this SOC 2 report is provided. You must promptly provide copies of such records to Microsoft or Deloitte & Touche LLP upon request. You must display or deliver the language in this paragraph or language that is substantially equivalent to this paragraph to recipients of this SOC 2 report for Microsoft Azure.

Microsoft

Microsoft Corporation - Azure Including Dynamics 365

(Azure & Azure Government)

System and Organization Controls (SOC) 2 Report

April 1, 2024 to March 31, 2025

Table of Contents

Executive Summary

Microsoft Azure	
Scope	Microsoft Azure, Microsoft Dynamics 365, and Microsoft Datacenters
Period of Examination	April 1, 2024 to March 31, 2025
Applicable Trust Services Criteria	Security, Availability, Processing Integrity, and Confidentiality
Additional Criteria	Bundesamt für Sicherheit in der Informationstechnik (BSI) Cloud Computing Compliance Criteria Catalogue (C5)
Datacenter Location(s)	**Americas** • West US • West US 2 • West US 3 • West Central US • Central US • USGOV Iowa • North Central US • USGOV Arizona • South Central US • USGOV Texas • East US • East US 2 • USGOV Virginia • USGOV Wyoming • Canada East • Canada Central • Mexico Central • Brazil South • Brazil Southeast **APAC** • Australia East • Australia Southeast • Australia Central • Australia Central 2 • New Zealand North • West India • Central India • Jio India West • Jio India Central • South India • East Asia • Japan West • Japan East • Southeast Asia • Korea South • Korea Central • Malaysia South • Taiwan North • Taiwan Northwest **EMEA** • West Europe • North Europe • UK South • UK West • France Central • France South • Germany North • Germany West Central • Spain Central • Switzerland West • Switzerland North • Norway East • Norway West • Qatar Central • Sweden Central • Sweden South • Poland Central • Italy North • South Africa North • South Africa West • UAE Central • UAE North • Israel Central

	Microsoft Azure
Edge Sites	• Athens, Greece (ATH01) • Atlanta, GA (ATA) • Auckland, New Zealand (AKL30) • Bangkok, Thailand (BKK30) • Barcelona, Spain (BCN30) • Barueri, Brazil (GRU30) • Berlin, Germany (BER30) • Bogota, Colombia (BOG30) • Brisbane, Australia (BNE01) • Brussels, Belgium (BRU30) • Bucharest, Romania (BUH01) • Budapest, Hungary (BUD01) • Buenos Aires, Argentina (BUE30) • Busan, South Korea (PUS03) • Cairo, Egypt (CAI30) • Cape Town, South Africa (CPT02/30) • Chicago, IL (CHG, CHI30) • Cincinnati, OH (CVG30) • Copenhagen, Denmark (CPH30) • Dallas, TX (DFW30) • Detroit, MI (DTT30) • Doha, Qatar (DOH30/31) • Dubai, United Arab Emirates (DXB30) • Dusseldorf, Germany (DUS30) • Frankfurt, Germany (FRA/31) • Geneva, Switzerland (GVA30) • Helsinki, Finland (HEL02) • Ho Chi Minh City, Vietnam (SGN30) • Hong Kong (HKB, HKG30) • Honolulu, HI (HNL01) • Houston, TX (HOU01) • Hyderabad, India (HYD30) • Istanbul, Turkey (IST30) • Jakarta, Indonesia (JKT30) • Jacksonville, FL (JAX30) • Johannesburg, South Africa (JNB02) • Kuala Lumpur, Malaysia (KUL30) • Luanda, Angola (LAD30) • Lisbon, Portugal (LIS01) • London, United Kingdom (LON04, LTS) • Los Angeles, CA (LAX) • Lagos, Nigeria (LOS30) • Madrid, Spain (MAD30) • Manchester, United Kingdom (MAN30/31) • Manila, Philippines (MNL30) • Memphis, TN (MEM30) • Miami, FL (MIA) • Milan, Italy (MIL30) • Minneapolis, MN (MSP30) • Montreal, Canada (YMQ01) • Mumbai, India (BOM02) • Munich, Germany (MUC30) • Nairobi, Kenya (NBO30) • Nashville, TN (BNA30) • New Delhi, India (DEL01) • New York City, NY (NYC) • Newark, NJ (EWR30) • Osaka, Japan (OSA30/31) • Oslo, Norway (OSL30) • Palo Alto, CA (PAO) • Paris, France (PRA) • Philadelphia, PA (PHL30) • Phoenix, AZ (PHX31) • Portland, OR (PDX31) • Prague, Czech Republic (PRG01) • Pune, India (PNQ30) • Queretaro, Mexico (MEX30/31) • Rabat, Morocco (RBA30) • Rio de Janeiro (RIO02/03) • Rome, Italy (ROM30) • Sao Paulo, Brazil (SAO31) • Salt Lake City, UT (SLC31) • Seattle, WA (WST, STB) • Seoul, South Korea (SLA) • Singapore (SGE, SIN30, SG1) • Sofia, Bulgaria (SOF01) • Stockholm, Sweden (STO) • Taipei, Taiwan (TPE30/31) • Tel Aviv, Israel (TLV30) • Teterboro, NJ (TEB31) • Tokyo, Japan (TYA/TYB) • Toronto, Canada (YTO01/30) • Warsaw, Poland (WAW01/30) • Zagreb, Croatia (ZAG30) • Zurich, Switzerland (ZRH)
Subservice Providers	N/A
Opinion Result	Unqualified
Testing Exceptions	10

Section 1:
Independent Service Auditor’s Report for the Security, Availability, Processing Integrity, and Confidentiality Criteria, and C5

Deloitte.

Deloitte & Touche LLP
1015 Second Avenue
Suite 500
Seattle, WA 98104
USA

Tel: 206-716-7000
www.deloitte.com

Section 1: 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[1] system of management of Microsoft Corporation (the "Service Organization" or "Microsoft") included in section 3, "Management of Microsoft's Description of its Azure System" throughout the period April 1, 2024 to March 31, 2025[2] (the "Description") based on the criteria for a Description of a service organization's system set forth in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*, in AICPA *Description Criteria,* ("description criteria"), and the suitability of the design and, operating effectiveness of controls stated in the Description throughout the period April 1, 2024 to March 31, 2025, 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")[3] 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 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 5, "Other Information Provided by Management of Microsoft" is presented by the management of Microsoft to provide additional information and is not a part of management of Microsoft's Description of its Azure system made available to user entities during the period April 1, 2024 to March 31, 2025. Content on the webpages directed by all the links and information in section 5 have not been subjected to the procedures applied in the examination of the Description of the Azure system and of the suitability of the design and operating effectiveness of the controls to achieve (a) Microsoft's service commitments and system

[1] Azure comprises of in-scope services and offerings for Microsoft Azure, Microsoft Dynamics 365, and Microsoft datacenters in the Azure and Azure Government cloud environments.

[2] In-scope services and offerings and coverage periods are defined in the *Azure and Azure Government Report Scope and Boundary,* and *Internal Supporting Services* subsections in section 3 of this SOC 2 report. Applicability of the Processing Integrity Trust Services Criteria is defined in the *Azure and Azure Government Report Scope and Boundary* subsection in section 3 of this SOC 2 report. In-scope datacenters, edge sites, and coverage periods are defined in the *Regions Covered by this Report* subsection in section 3 of this SOC 2 report.

[3] Applicable trust services criteria for Microsoft datacenters are Security and Availability.

requirements based on the applicable trust services criteria; and (b) the objectives set forth in C5 and, accordingly we express no opinion on it.

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 2 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.

Management of Microsoft is also responsible for selecting BSI C5 as additional criteria, and for implementing and operating effective controls to meet the requirements and the objectives set forth in the BSI C5.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the Description and on the suitability of the 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. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are also responsible for expressing an opinion about whether the controls stated in the Description were implemented and operated effectively to meet the requirements and the objectives set forth in the BSI C5 based on our examination. Attestations standards established by the AICPA require that we also plan and perform our examination to obtain reasonable assurance about whether, in all material respects, Microsoft implemented and operated effective controls to meet the requirements and the objectives set forth in the BSI C5 based on our examination. 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, the suitability of the design and operating effectiveness of those controls involves:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements and the objectives set forth in the BSI C5.
- 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 (a) the service organization would achieve its service commitments and system requirements based on the applicable trust services criteria; and (b) the objectives set forth in C5 would be achieved.

- Testing the operating effectiveness of those controls stated in the Description to provide reasonable assurance that (a) Microsoft achieved its service commitments and system requirements based on the applicable trust services criteria; and (b) the objectives set forth in C5 were achieved.
- 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 in any system of internal control, including the possibility of human error and the circumvention of controls.

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

Description of Tests of Controls

The specific controls we tested, and the nature, timing, and results of those tests are listed in section 4, "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."

Emphasis of a Matter - Cyber Incident

Microsoft has publicly acknowledged cyberattacks by a state-sponsored entity known as Midnight Blizzard. Passwords and other secrets were exfiltrated, allowing access to certain source code repositories, additional secrets, databases, and applications.

Based upon information known as of October 15, 2024, Microsoft acknowledged that certain passwords, secrets, and code repositories relevant to this report were accessed or exfiltrated. Microsoft represented that these passwords and secrets have been rotated or remediated. Microsoft also stated that code repository access gained by the threat actor was not and cannot be used to make production changes. We inspected certain listings provided by Microsoft of applications, resources, and code repositories impacted by these incidents, including those aligned to passwords and secrets that were accessed. We did not identify evidence that contradicts Microsoft's explanations and representations. Microsoft has determined that the incident was closed on October 15, 2024.

Opinion

In our opinion, in all material respects:

a. The Description presents Microsoft's Azure system that was designed and implemented throughout the period April 1, 2024 to March 31, 2025, in accordance with the description criteria.

b. The controls stated in the Description were suitably designed throughout the period April 1, 2024 to March 31, 2025, to provide reasonable assurance that Microsoft's service commitments and systems requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period.

c. The controls stated in the Description operated effectively throughout the period April 1, 2024 to March 31, 2025, to provide reasonable assurance that Microsoft's service commitments and system requirements would be achieved based on the applicable trust services criteria.

d. The controls stated in the Description operated effectively throughout the period April 1, 2024 to March 31, 2025, to provide reasonable assurance that Microsoft's service commitments and system requirements were achieved to meet the objectives set forth in the BSI C5.

Restricted Use

This report, including the description of tests of controls and results thereof in section 4, is intended solely for the information and use of management of Microsoft, user entities of Microsoft's Azure system during some or all of the period April 1, 2024 to March 31, 2025, business partners of Microsoft subject to risks arising from interactions with Microsoft's system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, regulators, or sponsoring organizations who developed C5 objectives, all of whom have sufficient knowledge and understanding of the following:

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

May 22, 2025

Section 2:
Management of Microsoft’s Assertion

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 706 7329
www.microsoft.com

Section 2: Management of Microsoft's Assertion

We have prepared the description of the Azure[4] system of management of Microsoft Corporation (the "Service Organization" or "Microsoft") included in section 3, "Management of Microsoft's Description of its Azure System" throughout the period April 1, 2024 to March 31, 2025[5] (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 (a) 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")[6] set forth in TSP Section 100, 2017 *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* in AICPA *Trust Services Criteria*; and (b) the objectives set forth in the Bundesamt für Sicherheit in der Informationstechnik (BSI) Cloud Computing Compliance Criteria Catalogue ("C5") were achieved.

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 April 1, 2024 to March 31, 2025, in accordance with the description criteria.

b. The controls stated in the Description were suitably designed throughout the period April 1, 2024 to March 31, 2025, 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.

c. The controls stated in the Description operated effectively throughout the period April 1, 2024 to March 31, 2025, to provide reasonable assurance that Microsoft's service commitments and system requirements were achieved based on the applicable trust services criteria.

d. The controls stated in the Description operated effectively throughout the period April 1, 2024 to March 31, 2025, to provide reasonable assurance that Microsoft's service commitments and system requirements were achieved to meet the objectives set forth in the BSI C5.

[4] Azure comprises of in-scope services and offerings for Microsoft Azure, Microsoft Dynamics 365, and Microsoft datacenters in the Azure and Azure Government cloud environments.

[5] In-scope services and offerings and coverage periods are defined in the *Azure and Azure Government Report Scope and Boundary,* and *Internal Supporting Services* subsections in section 3 of the SOC 2 report. Applicability of the Processing Integrity Trust Services Criteria is defined in the *Azure and Azure Government Report Scope and Boundary* subsection in section 3 of the SOC 2 report. In-scope datacenters, edge sites, and coverage periods are defined in the *Regions Covered by this Report* subsection in section 3 of the SOC 2 report.

[6] Applicable trust services criteria for Microsoft datacenters are Security and Availability.

Section 3:
Management of Microsoft’s Description of its Azure System

Section 3: Management of Microsoft’s Description of its Azure System

Overview of Operations

Business Description

Azure

Microsoft Azure is a cloud computing platform for building, deploying and managing applications through a global network of Microsoft and third-party managed datacenters. It supports both Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) cloud service models and enables hybrid solutions that integrate cloud services with customers’ on-premises resources. Microsoft Azure supports many customers, partners, and government organizations that span across a broad range of products and services, geographies, and industries. Microsoft Azure is designed to meet their security, confidentiality, and compliance requirements.

Microsoft datacenters support Microsoft Azure, Microsoft Dynamics 365, and Microsoft Online Services (“Online Services”). Online Services such as Intune, Power BI, and others are Software as a Service (SaaS) services that leverage the underlying Microsoft Azure platform and datacenter infrastructure. See section titled ‘Azure and Azure Government Report Scope and Boundary’ for the Microsoft Azure services and offerings and Online Services that are in scope for this report.

Dynamics 365

Dynamics 365 is an online business application suite that integrates the Customer Relationship Management (CRM) capabilities and its extensions with the Enterprise Resource Planning (ERP) capabilities. These end-to-end business applications help customers turn relationships into revenue, earn customers, and accelerate business growth.

“Azure”, when referenced in this report, comprises of “Microsoft Azure”, “Microsoft Dynamics 365”, “Online Services”, and the supporting datacenters listed in this report.

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 services. 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 the underlying physical and virtual infrastructure of the Azure services and offerings

Trust Services Criteria	Description	Applicability Considerations
Availability	Addresses risks related to system accessibility for processing, monitoring and maintenance	Applies to the Azure services and offerings whose accessibility is advertised or committed by contract
Processing Integrity	Addresses risks related to completeness, accuracy, and timeliness of system / application processing of transactions	Applies to the Azure services and offerings that operate transaction processing interfaces
Confidentiality	Addresses risks related to unauthorized access or disclosure of specific information designated as "confidential" within contractual arrangements	Applies to the customer data elements that are designated as "confidential" based on Azure's data classification policy
Privacy	Addresses risks related to protection and management of personal information	Privacy of end-users and any privacy-related data associated with applications or services developed on the Azure platform is the customer's responsibility as described in Microsoft Trust Center Not applicable since personal information of customer administrators is collected and handled within Microsoft Online Customer Portal (MOCP), which is outside the scope of the Azure system boundaries

As such, the detail herein is limited to operational controls supporting Azure and Online Services as defined in the Azure and Azure Government Report Scope and Boundary described below. Azure services and offerings and supported Online Services in scope for this report are defined separately for the following environments: Azure and Azure Government.

Azure and Azure Government Report Scope and Boundary

Azure is global multi-tenant cloud platform that provides a public cloud deployment model. Azure Government is a US Government Community Cloud that is physically separated from the Azure cloud. The following Azure and Azure Government services and offerings are in scope for this report:

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[7]	
		Azure	Azure Government	H1 FY25	H2 FY25
Microsoft Datacenters					
Microsoft Datacenter and Operations Service		✓	✓	✓	✓
Azure					
Compute	Azure App Service	✓	✓	✓	✓
	Azure Arc	✓	✓	✓	✓
	Azure Cloud Services[8]	✓	✓	✓	✓
	Azure Cloud Services (Extended Support)	✓	✓	✓	✓
	Azure Functions	✓	✓	✓	✓
	Azure Large Instances	✓	-	✓	✓
	Azure Machine Configuration	✓	✓	✓	✓
	Azure Service Fabric	✓	✓	✓	✓
	Azure Virtual Desktop	✓	✓	✓	✓
	Azure Virtual Machines	✓	✓	✓	✓
	Azure Virtual Machine Scale Sets	✓	✓	✓	✓
	Azure VM Image Builder	✓	-	✓	✓
	Azure VMware Solution	✓	✓	✓	✓
	Batch	✓	✓	✓	✓
	Planned Maintenance	✓	✓	✓	✓
	Virtual Machines Licenses	✓	-	-	✓
Containers	Azure Arc Enabled Kubernetes	✓	✓	✓	✓

[7] Examination period scope H1 FY25 extends from April 1, 2024 to September 30, 2024.
Examination period scope H2 FY25 extends from October 1, 2024 to March 31, 2025.

[8] Offerings for which AICPA Processing Integrity trust service criteria were examined: Azure Cloud Services, Azure Resource Manager (ARM), Microsoft Azure Portal and Azure Service Manager (RDFE).

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[7]	
		Azure	Azure Government	H1 FY25	H2 FY25
	Azure Container Apps[9]	✓	✓	✓	✓
	Azure Container Instances	✓	✓	✓	✓
	Azure Container Registry	✓	✓	✓	✓
	Azure Kubernetes Configuration Management	✓	✓	✓	✓
	Azure Kubernetes Service (AKS)	✓	✓	✓	✓
	Azure Red Hat OpenShift	✓	✓	✓	✓
	Microsoft Artifact Registry	✓	-	✓	✓
Networking	Application Gateway	✓	✓	✓	✓
	Azure Bastion	✓	✓	✓	✓
	Azure Communications Gateway	✓	-	✓	✓
	Azure Content Delivery Network	✓	✓	✓	✓
	Azure DDoS Protection	✓	✓	✓	✓
	Azure DNS	✓	✓	✓	✓
	Azure ExpressRoute	✓	✓	✓	✓
	Azure Firewall	✓	✓	✓	✓
	Azure Firewall Manager	✓	✓	✓	✓
	Azure Front Door	✓	✓	✓	✓
	Azure Load Balancer	✓	✓	✓	✓
	Azure NAT Gateway	✓	✓	✓	✓
	Azure Network Function Manager	✓	✓	-	✓

[9] Examination period for this offering / service for Azure public instance was from April 1, 2024 to March 31, 2025, while the examination period for this offering / service for Azure Government instance was from October 1, 2024, to March 31, 2025.

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[7]	
		Azure	Azure Government	H1 FY25	H2 FY25
	Azure Orbital Ground Station	✓	-	✓	✓
	Azure Peering Service	✓	✓	✓	✓
	Azure Private Link	✓	✓	✓	✓
	Azure Private MEC	✓	-	✓	-
	Azure Route Server	✓	✓	✓	✓
	Azure Traffic Collector	✓	-	✓	✓
	Azure Virtual Network	✓	✓	✓	✓
	Azure Virtual Network IP Services	✓	✓	✓	✓
	Azure Virtual Network Manager	✓	-	✓	✓
	Azure Web Application Firewall	✓	✓	✓	✓
	Network Watcher	✓	✓	✓	✓
	Traffic Manager	✓	✓	✓	✓
	Virtual WAN	✓	✓	✓	✓
	VPN Gateway	✓	✓	✓	✓
Storage	Azure Archive Storage	✓	✓	✓	✓
	Azure Backup	✓	✓	✓	✓
	Azure Data Box	✓	✓	✓	✓
	Azure File Sync	✓	✓	✓	✓
	Azure Files	✓	✓	-	✓
	Azure HPC Cache	✓	✓	✓	✓
	Azure Managed Lustre	✓	✓	✓	✓
	Azure NetApp Files	✓	✓	✓	✓
	Azure Site Recovery	✓	✓	✓	✓

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[7]	
		Azure	Azure Government	H1 FY25	H2 FY25
	Azure Storage (Blobs (including Azure Data Lake Storage Gen2), Disks, Files, Queues, Tables, Azure Disk Storage) including Cool and Premium	✓	✓	✓	✓
	Azure Storage Mover	✓	-	✓	✓
Databases	Azure Cache for Redis	✓	✓	✓	✓
	Azure Cosmos DB	✓	✓	✓	✓
	Azure Database for MariaDB	✓	✓	✓	✓
	Azure Database for MySQL	✓	✓	✓	✓
	Azure Database for PostgreSQL	✓	✓	✓	✓
	Azure Database Migration Service	✓	✓	✓	✓
	Azure Health Data Services	✓	✓	✓	✓
	Azure SQL	✓	✓	✓	✓
	Azure SQL Managed Instance	✓	✓	✓	✓
	Azure Synapse Analytics	✓	✓	✓	✓
	Microsoft Azure Managed Instance for Apache Cassandra	✓	-	✓	✓
	SQL Managed Instance enabled by Azure Arc	✓	-	✓	✓
	SQL Server enabled by Azure Arc	✓	-	✓	✓
	SQL Server on Azure Virtual Machines	✓	✓	✓	✓
	SQL Server Stretch Database	✓	✓	✓	-
Developer Tools	Azure App Configuration	✓	✓	✓	✓
	Azure Deployment Environments	✓	-	✓	✓

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[7]	
		Azure	Azure Government	H1 FY25	H2 FY25
	Azure DevTest Labs	✓	✓	✓	✓
	Azure for Education	✓	-	✓	✓
	Azure Lab Services	✓	-	✓	✓
	Azure Load Testing	✓	-	✓	✓
	Azure Managed Grafana	✓	-	✓	✓
	Microsoft Dev Box	✓	-	✓	✓
	Service Connector	✓	-	✓	✓
Analytics	Azure Analysis Services	✓	✓	✓	✓
	Azure Chaos Studio	✓	-	✓	✓
	Azure Data Explorer	✓	✓	✓	✓
	Azure Data Factory	✓	✓	✓	✓
	Azure Data Share	✓	✓	✓	✓
	Azure HDInsight	✓	✓	✓	✓
	Azure Operator Insights	✓	-	✓	-
	Azure Stream Analytics	✓	✓	✓	✓
	Data Catalog	✓	-	✓	-
	Data Lake Analytics	✓	-	✓	-
	Healthcare data solutions in Microsoft Fabric	✓	-	-	✓
	Microsoft Fabric	✓	-	✓	✓
	Power BI Embedded	✓	✓	✓	✓
AI + Machine Learning	AI Builder	✓	✓	✓	✓
	Azure AI Foundry Portal	✓	-	-	✓
	Azure AI Services	✓	✓	✓	✓
	Azure AI Services: AI Anomaly Detector	✓	-	✓	✓

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[7]	
		Azure	Azure Government	H1 FY25	H2 FY25
	Azure AI Services: Azure AI Containers	✓	✓	✓	✓
	Azure AI Services: Azure AI Content Safety	✓	✓	✓	✓
	Azure AI Services: Azure AI Custom Vision	✓	✓	✓	✓
	Azure AI Services: Azure AI Document Intelligence	✓	✓	✓	✓
	Azure AI Services: Azure AI Face Service	✓	✓	✓	✓
	Azure AI Services: Azure AI Immersive Reader	✓	-	✓	✓
	Azure AI Services: Azure AI Language	✓	-	✓	✓
	Azure AI Services: Azure AI Metrics Advisor	✓	-	✓	✓
	Azure AI Services: Azure AI Personalizer	✓	✓	✓	✓
	Azure AI Services: Azure AI Search	✓	✓	✓	✓
	Azure AI Services: Azure AI Speech	✓	✓	✓	✓
	Azure AI Services: Azure AI Translator	✓	✓	✓	✓
	Azure AI Services: Azure AI Video Indexer	✓	✓	✓	✓
	Azure AI Services: Azure AI Vision	✓	✓	✓	✓
	Azure AI Services: Conversational Language Understanding	✓	✓	✓	✓
	Azure AI Services: Question Answering	✓	✓	✓	✓
	Azure AI Bot Service	✓	✓	✓	✓
	Azure Health Bot	✓	-	✓	✓
	Azure Open Datasets	✓	✓	✓	✓

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[7]	
		Azure	Azure Government	H1 FY25	H2 FY25
	Azure OpenAI Service	✓	✓	✓	✓
	Azure Machine Learning	✓	✓	✓	✓
	Copilot for Service	✓	-	-	✓
	Machine Learning Studio (Classic)	✓	-	✓	-
	Microsoft 365 Copilot for Sales	✓	-	✓	✓
	Microsoft Genomics	✓	-	✓	✓
	Seeing AI	✓	-	✓	✓
Internet of Things	Azure Digital Twins	✓	-	✓	✓
	Azure Event Grid	✓	✓	✓	✓
	Azure IoT Central	✓	-	✓	✓
	Azure IoT Hub	✓	✓	✓	✓
	Azure Sphere	✓	-	✓	✓
	Azure Time Series Insights	✓	-	✓	✓
	Device Update for IoT Hub	✓	-	✓	✓
	Event Hubs	✓	✓	✓	✓
	Microsoft Cloud for Sustainability	✓	-	✓	✓
	Microsoft Defender for IoT	✓	✓	✓	✓
	Notification Hubs	✓	✓	✓	✓
Integration	API Management	✓	✓	✓	✓
	Azure Data Manager for Energy	✓	-	✓	✓
	Azure Logic Apps	✓	✓	✓	✓
	Azure Service Bus	✓	✓	✓	✓
	Universal Print	✓	✓	✓	✓
Identity	Azure Active Directory B2C	✓	-	✓	✓

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[7]	
		Azure	Azure Government	H1 FY25	H2 FY25
	Microsoft Entra Domain Services	✓	✓	✓	✓
	Microsoft Entra ID	✓	✓	✓	✓
	Microsoft Entra Permissions Management	✓	-	✓	✓
	Microsoft Global Secure Access	✓	-	✓	✓
	Microsoft Purview Information Protection	✓	✓	✓	✓
Management and Governance	Application Change Analysis	✓	-	✓	✓
	Automation	✓	✓	✓	✓
	Azure Advisor	✓	✓	✓	✓
	Azure Blueprints	✓	✓	✓	✓
	Azure Lighthouse	✓	✓	✓	✓
	Azure Managed Applications	✓	✓	✓	✓
	Azure Migrate	✓	✓	✓	✓
	Azure Monitor	✓	✓	✓	✓
	Azure Policy	✓	✓	✓	✓
	Azure Quotas	✓	✓	✓	✓
	Azure Resource Graph	✓	✓	✓	✓
	Azure Resource Manager (ARM)[8]	✓	✓	✓	✓
	Azure Resource Mover	✓	✓	✓	✓
	Azure Signup Portal	✓	✓	✓	✓
	Azure Update Manager	✓	✓	-	✓
	Cloud Shell	✓	✓	✓	✓
	Cost Management	✓	✓	✓	✓
	Microsoft Azure Portal[8]	✓	✓	✓	✓
	Microsoft Purview (Governance)[9]	✓	✓	✓	✓

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[7]	
		Azure	Azure Government	H1 FY25	H2 FY25
Security	Azure Confidential Computing	✓	-	✓	✓
	Azure Confidential Ledger	✓	-	✓	✓
	Azure Dedicated HSM	✓	✓	✓	✓
	Azure Payment HSM	✓	-	✓	✓
	Customer Lockbox for Microsoft Azure	✓	✓	✓	✓
	Key Vault	✓	✓	✓	✓
	Microsoft Azure Attestation	✓	-	✓	✓
	Microsoft Copilot for Security	✓	-	✓	✓
	Microsoft Defender Experts for Hunting	✓	-	✓	✓
	Microsoft Defender Experts for XDR	✓	-	✓	✓
	Microsoft Defender for Cloud	✓	✓	✓	✓
	Microsoft Defender Threat Intelligence	✓	-	✓	✓
	Microsoft Sentinel	✓	✓	✓	✓
	Multi-Factor Authentication	✓	✓	✓	✓
	Windows Autopatch	✓	-	✓	✓
Media	Azure Media Services	✓	✓	✓	✓
Web	Azure Fluid Relay	✓	✓	✓	✓
	Azure Maps	✓	✓	✓	✓
	Azure SignalR Service	✓	✓	✓	✓
	Azure Spring Apps	✓	-	✓	✓
	Azure Web PubSub	✓	✓	✓	✓
Mixed Reality	Remote Rendering	✓	-	✓	✓
	Spatial Anchors	✓	-	✓	-

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[7]	
		Azure	Azure Government	H1 FY25	H2 FY25
Hybrid + MultiCloud	Azure Arc enabled System Center Virtual Machine Manager	✓	-	✓	✓
	Azure Arc enabled VMware vSphere	✓	-	✓	✓
	Azure Center for SAP Solutions	✓	-	✓	✓
	Azure Kubernetes Service on AzureStack HCI	✓	-	✓	✓
	Azure Operator Nexus	✓	-	✓	✓
	Azure Operator Service Manager	✓	-	✓	✓
	Azure Monitor for SAP Solutions	✓	-	✓	✓
Internal Supporting Services[8,10]		✓	✓	✓	✓

[10] Azure Government scope boundary for internal services: Access Monitoring, Asimov Event Forwarder, Atlas, Autopilot Security, AzCP Platform, Azure Diagnostic Services, Azure Notebooks Component, Azure Security Monitoring (ASM SLAM), Azure Service Health, Azure Stack Bridge, Azure Stack Diagnostics and Analytics Service, Azure Stack Edge Service, Azure Support Center, Azure System Lockdown, Azure Throttling Solutions, Azure Watson, CoreWAN, dSCM, dSMS, dSTS, DataGrid, Dynamics 365 Integrator App, Fabric Controller Fundamental Services, Fabric Network Devices, Gateway Manager, Geneva Actions, Geneva Analytics Orchestration, Geneva Warm Path, Interflow, JIT, MDM, MEE Privacy Service, Microsoft Bot Framework, Microsoft Email Orchestrator, MSaaS File Management (DTM V2), MSFT.RR DNS, Network Billing, OneBranch Release, OneDeploy Deployment Infrastructure (DE), OneDS Collector, PF-FC, Pilotfish, PMI Foundation, Resource Provider Service as a Service, Unified Remote Scanning (URSA), Vulnerability Scanning & Analytics, WaNetMon, Windows Azure Jumpbox, and Workflow. The coverage period for internal services for both Azure and Azure Government is April 1, 2024 through March 31, 2025 except for those specified with shorter coverage periods in the *Internal Supporting Services* subsection herein.

Offering	Cloud Environment Scope		Examination Period Scope[7]	
	Azure	Azure Government	H1 FY25	H2 FY25
Microsoft Online Services				
Appsource	✓	-	✓	✓
Dynamics 365 Customer Voice	✓	-	✓	✓
Endpoint Attack Notifications	✓	-	✓	✓
Intelligent Recommendations	✓	-	✓	✓
Microsoft Copilot Studio	✓	✓	✓	✓
Microsoft Defender for Cloud Apps	✓	✓	✓	✓
Microsoft Defender for Endpoint	✓	✓	✓	✓
Microsoft Defender for Identity	✓	✓	✓	✓
Microsoft Graph	✓	✓	✓	✓
Microsoft Intune	✓	✓	✓	✓
Microsoft Managed Desktop	✓	-	✓	✓
Microsoft Stream	✓	✓	✓	✓
Nomination Portal	✓	-	✓	-
Power Apps	✓	✓	✓	✓
Power Automate	✓	✓	✓	✓
Power BI	✓	✓	✓	✓
Windows Update for Business reports	✓	-	✓	✓

Offering	Cloud Environment Scope		Examination Period Scope[7]	
	Azure	Azure Government	H1 FY25	H2 FY25
Microsoft Dynamics 365				
Chat for Dynamics 365	✓	✓	✓	✓
Dataverse	✓	✓	✓	✓
Dynamics 365 AI Customer Insights	✓	✓	✓	✓
Dynamics 365 Athena - CDS to Azure Data Lake	✓	✓	✓	✓

Offering	Cloud Environment Scope		Examination Period Scope[7]	
	Azure	Azure Government	H1 FY25	H2 FY25
Dynamics 365 Business Central	✓	-	✓	✓
Dynamics 365 Commerce	✓	-	✓	✓
Dynamics 365 Contact Center	✓	-	✓	✓
Dynamics 365 Customer Insights - Data	✓	-	✓	✓
Dynamics 365 Customer Insights - Journeys	✓	-	✓	✓
Dynamics 365 Customer Service	✓	✓	✓	✓
Dynamics 365 Field Service	✓	✓	✓	✓
Dynamics 365 Finance	✓	✓	✓	✓
Dynamics 365 Fraud Protection	✓	-	✓	✓
Dynamics 365 Guides	✓	-	✓	✓
Dynamics 365 Human Resources	✓	-	✓	-
Dynamics 365 Intelligent Order Management	✓	-	✓	✓
Dynamics 365 Project Operations	✓	-	✓	✓
Dynamics 365 Remote Assist	✓	-	✓	✓
Dynamics 365 - Resource Scheduling Optimization	✓	✓	✓	✓
Dynamics 365 Sales	✓	✓	✓	✓
Dynamics 365 Sales Insights	✓	-	✓	✓
Dynamics 365 Supply Chain Management[9]	✓	✓	✓	✓
Microsoft Power Platform on Azure	✓	✓	✓	✓
Nuance Conversational IVR[9]	✓	✓	✓	✓
Power Pages	✓	✓	✓	✓

Offering	Cloud Environment Scope		Examination Period Scope[7]	
	Azure	Azure Government	H1 FY25	H2 FY25
Microsoft Cloud for Financial Services				
Unified Customer Profile	✓	-	✓	-
Collaboration Manager	✓	-	✓	-
Customer Onboarding	✓	-	✓	-

Regions Covered by this Report

Azure production infrastructure is located in globally distributed datacenters. These datacenters across multiple regions deliver the core physical infrastructure that includes physical hardware asset management, security, data protection, networking services. These datacenters are managed, monitored, and operated by Microsoft operations staff delivering online services with 24x7 continuity. The purpose-built facilities are part of a network of datacenters that provide mission critical services to Azure and other Online Services. The datacenters in scope for the purposes of this report are:

Azure Regions

Americas

- West US
- West US 2
- West US 3
- West Central US
- Central US
- USGOV Iowa
- North Central US
- USGOV Arizona
- South Central US
- USGOV Texas
- East US
- East US 2
- USGOV Virginia
- USGOV Wyoming
- Canada East
- Canada Central
- Mexico Central
- Brazil South
- Brazil Southeast

APAC

- Australia East
- Australia Southeast
- Australia Central
- Australia Central 2
- New Zealand North[11]
- West India
- Central India
- Jio India West
- Jio India Central
- South India
- East Asia
- Japan West
- Japan East
- Southeast Asia
- Korea South
- Korea Central
- Malaysia South
- Taiwan North
- Taiwan Northwest

EMEA

- West Europe
- North Europe
- UK South
- UK West
- France Central
- France South
- Germany North
- Germany West Central
- Spain Central
- Switzerland West
- Switzerland North
- Norway East
- Norway West
- Qatar Central
- Sweden Central
- Sweden South
- Poland Central
- Italy North
- South Africa North
- South Africa West
- UAE Central
- UAE North
- Israel Central

In addition to the datacenters included in the Azure regions listed above, there are datacenters outside of those regions which are included in the scope of the examination and are supporting Microsoft 365 services. Note that the Microsoft 365 services are not included in the scope of the examination.

[11] Examination period for the Azure region was from October 1, 2024 to March 31, 2025.

Edge Sites

- Athens, Greece (ATH01)
- Atlanta, GA (ATA)[12]
- Auckland, New Zealand (AKL30)
- Bangkok, Thailand (BKK30)
- Barcelona, Spain (BCN30)
- Barueri, Brazil (GRU30)
- Berlin, Germany (BER30)
- Bogota, Colombia (BOG30)
- Brisbane, Australia (BNE01)
- Brussels, Belgium (BRU30)
- Bucharest, Romania (BUH01)
- Budapest, Hungary (BUD01)
- Buenos Aires, Argentina (BUE30)
- Busan, South Korea (PUS03)[12]
- Cairo, Egypt (CAI30)
- Cape Town, South Africa (CPT30)
- Chicago, IL (CHG, CHI30)
- Cincinnati, OH (CVG30)
- Copenhagen, Denmark (CPH30)
- Dallas, TX (DFW30)
- Detroit, MI (DTT30)
- Doha, Qatar (DOH30/31[12])
- Dubai, United Arab Emirates (DXB30)
- Dusseldorf, Germany (DUS30)
- Frankfurt, Germany (FRA/31)
- Geneva, Switzerland (GVA30)
- Helsinki, Finland (HEL02)
- Ho Chi Minh City, Vietnam (SGN30)
- Hong Kong (HKB, HKG30)[12]
- Honolulu, HI (HNL01)
- Houston, TX (HOU01)
- Hyderabad, India (HYD30)
- Istanbul, Turkey (IST30)
- Jakarta, Indonesia (JKT30)
- Jacksonville, FL (JAX30)
- Johannesburg, South Africa (JNB02)
- Kuala Lumpur, Malaysia (KUL30)
- Luanda, Angola (LAD30)
- Lisbon, Portugal (LIS01)
- London, United Kingdom (LON04, LTS)
- Los Angeles, CA (LAX)
- Lagos, Nigeria (LOS30)
- Madrid, Spain (MAD30)
- Manchester, United Kingdom (MAN30/31)
- Manila, Philippines (MNL30)
- Memphis, TN (MEM30)
- Miami, FL (MIA)
- Milan, Italy (MIL30)
- Minneapolis, MN (MSP30)
- Montreal, Canada (YMQ01)
- Mumbai, India (BOM02)
- Munich, Germany (MUC30)
- Nairobi, Kenya (NBO30)
- Nashville, TN (BNA30)
- New Delhi, India (DEL01)
- New York City, NY (NYC)
- Newark, NJ (EWR30)
- Osaka, Japan (OSA30/31)
- Oslo, Norway (OSL30)
- Palo Alto, CA (PAO)
- Paris, France (PRA, PAR02)
- Philadelphia, PA (PHL30)
- Phoenix, AZ (PHX31)
- Portland, OR (PDX31)
- Prague, Czech Republic (PRG01)
- Pune, India (PNQ30)
- Queretaro, Mexico (MEX30/31)
- Rabat, Morocco (RBA30)
- Rio de Janeiro (RIO02/03)
- Rome, Italy (ROM30)
- Sao Paulo, Brazil (SAO31)
- Salt Lake City, UT (SLC31)
- Seattle, WA (WST, STB)
- Seoul, South Korea (SLA)
- Singapore (SGE[12], SIN30, SG1)
- Sofia, Bulgaria (SOF01)
- Stockholm, Sweden (STO)
- Taipei, Taiwan (TPE30/31)
- Tel Aviv, Israel (TLV30)
- Teterboro, NJ (TEB31)
- Tokyo, Japan (TYA/TYB)
- Toronto, Canada (YTO01/30)
- Warsaw, Poland (WAW01/30)
- Zagreb, Croatia (ZAG30)
- Zurich, Switzerland (ZRH)

[12] Examination period for the Edge Site was from April 1, 2024 to September 30, 2024.

In addition to datacenter, network, and personnel security practices, Azure also incorporates security practices at the application and platform layers to enhance security for application development and service administration.

Principal Service Commitments and System Requirements

Microsoft makes service commitments to its customers, business partners and vendors, and has established system requirements as part of the Azure 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 the Microsoft Online Subscription Agreement, Product Terms, Microsoft Azure 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 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.

- 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 including the following:

- Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained.
- In addition to these policies, standard operating procedures are documented on how to carry out specific manual and automated processes required in the operation and development of various Azure services and offerings.
- Procedures are in place so that the access, collection, use, and deletion of customer data is in accordance with the service commitments.
- Cryptographic controls are implemented to protect customer data. Access to cryptographic keys is restricted to only authorized personnel.
- 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 and communicated.
- Azure services are designed to maintain high availability through redundancy and automatic failover to minimize disruption to services.
- Critical systems are monitored through third-party and internal tools to maintain availability.

- Access to physical and logical assets is limited to authorized users and is provisioned based on job requirements to mitigate risk of unauthorized access.
- Automated logging and alerting capabilities are implemented for Azure services to detect potential unauthorized activity and security events.
- Incidents impacting internal and customer systems are detected, escalated and resolved.
- Development of new features and major changes to Azure services are performed in accordance with policies and procedures.
- Azure offerings and services are configured be interoperable with industry standards.

Such requirements are communicated in Azure's system policies and procedures, system design documentation, and contracts with customers. Microsoft's service commitments and system requirements are designed based on the trust services criteria relevant to security, availability, processing integrity, and confidentiality, and other frameworks.

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 across 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 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. SBC was developed in full consideration of Sarbanes-Oxley Act (SOX) 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 in which Microsoft operates. It also guides employees and contingent staff on the processes and channels available to report possible violations or to ask questions. Microsoft also trains its outsourced providers to understand and comply with Microsoft's supplier code of conduct.

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 environment and datacenters are also accountable for understanding and adhering to the guidance contained in the Security Policy and standards.

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. These Core Priorities are established when an employee is hired, and then updated during one-on-one Connect meetings with their manager. The primary focus of the Connect meetings is to assess employee performance against their priorities and to agree on an updated list of priorities going forward.

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.

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.

Compliance & Ethics - Board of Directors and Senior Leadership

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

Internal Audit Department

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

Audit Committee

The AC charter and responsibilities are 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) team provides management and accountability of Microsoft Corporate's short- and long-term risks. ERM collaborates with Internal Audit, the Financial Compliance Group, Operations, and Legal and Compliance groups to perform a formal risk assessment. These risk assessments include risks in financial reporting, fraud, and compliance with laws.

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 are uncovered are 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 Resource (HR), Finance, Procurement, and others to determine specific fraud risks and responses.

Periodic Risk Assessment

IA 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 risks related to financial reporting, operational business process, and systems controls. Control failures are also assessed to determine whether they give rise to additional risks.

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

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

Monitoring

Security and Compliance Monitoring

Azure and the datacenters maintain 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.

Compliance & 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 Compliance & Ethics - Business & Regulatory Investigations team.

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 midyear review process.

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 toward sound internal controls. The Office of the CFO is responsible for a number of communications outside the company, including Quarterly Earnings Release, Financial Analyst meetings, customer visits, external conferences, and external publications.

Data

Customers upload data for storage or processing within the services or applications that are hosted on the cloud services platform. In addition, certain types of data are provided by the customers or generated on the customer’s behalf to enable the usage of the cloud services. Microsoft only uses customer data in order to support the provisioning of the services subscribed to by the customers in accordance with the Service Level Agreements (SLAs). The customer provided data are broadly classified into the following data types:

1. **Access Control Data** is data used to manage access to administrative roles or sensitive functions.
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 in a Microsoft Online Service or product.
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 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. **Managed Service** Data is all data provided to Microsoft by the Managed Service customer and / or the Managed Service personnel as part of a Managed Service engagement.
10. **Organization Identifiable Information (OII)** is data that can be used to identify a particular tenant / Azure subscription / deployment / organization (generally configuration or usage data) and is not linkable to a user.

11. **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.

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

Data Ownership

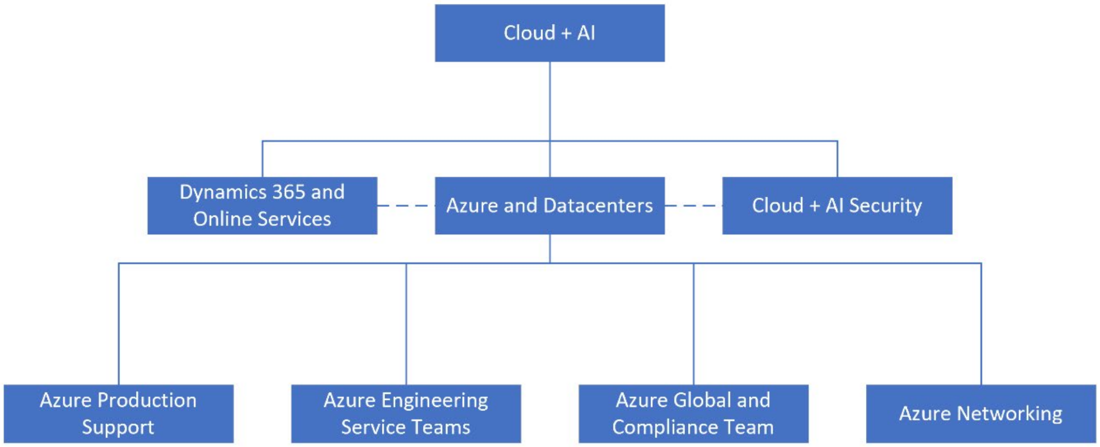
Microsoft does not inspect, approve, or monitor applications that customers deploy to Azure. Moreover, Microsoft does not know what kind of data customers choose to store in Azure. Microsoft does not claim data ownership over the customer information entered into Azure. Azure's Agreement states, "Customers are solely responsible for the content of all Customer Data. Customers will secure and maintain all rights in Customer Data necessary for Azure to provide the Online Services to them without violating the rights of any third party or otherwise obligating Microsoft to them or to any third party. Microsoft does not and will not assume any obligations with respect to Customer Data or to their use of the Product other than as expressly set forth in the Agreement or as required by applicable law."

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.

People

Azure is comprised and supported by the following groups who are responsible for the delivery and management of Azure services:


Cloud + AI
Dynamics 365 and Online Services
Azure and Datacenters
Cloud + AI Security
Azure Production Support
Azure Engineering Service Teams
Azure Global and Compliance Team
Azure Networking

Online, Infrastructure, and Platform Services

Online services are software hosted in Azure Engineering Service teams managed production subscriptions for the purpose of making an Azure offering available or delivering features and capabilities to the Azure product. Infrastructure services manage the data center hardware that is essential for Azure services to run. Platform services manage the availability and features of a platform on which an Azure online service is hosted. Altogether, Online, Infrastructure, and Platform services manage the service lifecycle of the finished PaaS, SaaS, and IaaS Azure offerings.

Cloud + AI Security

The Cloud + AI Security team works to make Azure a secure and compliant cloud platform by building common security technologies, tools, processes, and best practices. The Cloud + AI Security team is involved in the review of deployments and enhancements of Azure services to facilitate security considerations at every level of the Security Development Lifecycle (SDL). They also perform security reviews and provide security guidance for the datacenters. This team consists of personnel responsible for:

- Security Development Lifecycle
- Security incident response
- Driving security functionality within service development work

Azure Production Support

The Azure Production Support team is responsible for build-out, deployment and management of Azure services. This team consists of the following:

- **Azure Live Site** - Monitors and supports the Azure platform; proactively addresses potential platform issues; and reacts to incidents and support requests
- **Azure Deployment Engineering** - Builds out new capacity for the Azure platform; and deploys platform and product releases through the release pipeline
- **Azure Customer Support** - Provides support to individual customers and multinational enterprises from basic break-fix support to rapid response support for mission critical applications

Azure Engineering Service Teams

The Azure Engineering Service teams manage the service lifecycle. Their responsibilities include:

- Development of new services
- Serving as an escalation point for support
- Providing operational support for existing services (DevOps model)

The team includes personnel from the Development, Test and Program Management (PM) disciplines for design, development, and testing of services, and providing technical support as needed.

Global Ecosystem and Compliance Team

The Global Ecosystem and Compliance team is responsible for developing, maintaining and monitoring the Information Security (IS) program including the ongoing risk assessment process.

As part of managing compliance adherence, the team drives related features within the Azure product families. This team consists of personnel responsible for:

- Training
- Privacy
- Risk assessment
- Internal and external audit coordination

Networking

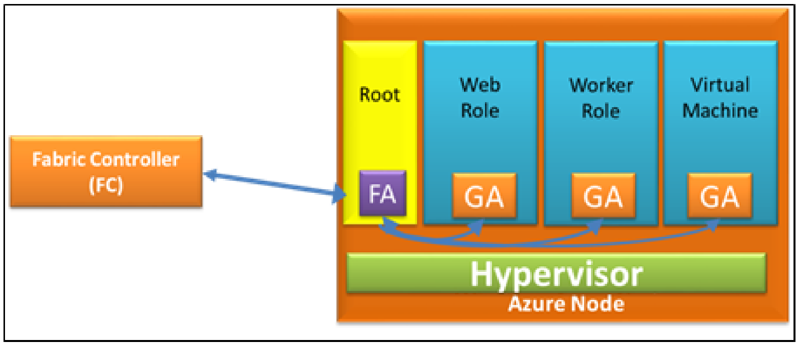
The Networking team is responsible for implementing, monitoring and maintaining the Microsoft network. This team consists of personnel responsible for:

- Network configuration and access management
- Network problem management
- Network capacity management

Azure Environment

Azure is developed and managed by the Azure team, and provides a cloud platform based on machine virtualization. This means that customer code - whether it's deployed in a PaaS Worker Role or an IaaS Virtual Machine - executes in a Windows Server Hyper-V virtual machine. Every physical node in Azure has one or more virtual machines, also called instances, that are scheduled on physical CPU cores, are assigned dedicated RAM, and have controlled access to local disk and network I/O.

On each Azure node, there is a Hypervisor that runs directly over the hardware and divides a node into a variable number of Guest Virtual Machines (VMs). Each node also has one special Root VM, which runs the Host Operating System (OS), as shown in figure below. Fabric Agents (FAs) on Root VMs are used to manage Guest Agents (GAs) within Guest VMs. Isolation of the Root VM from the Guest VMs and the Guest VMs from one another is a key concept in Azure security architecture.



Fabric Controller Lifecycle Management

In Azure, VMs (nodes) run on groups of physical servers known as "clusters", of approximately 1,000 machines. Each cluster is independently managed by a scaled-out and redundant platform Fabric Controller (FC) software component.

Each FC manages the lifecycle of VMs and applications running in its cluster, including provisioning and monitoring the health of the hardware under its control. The FC executes both automatic operations, like healing VM instances to healthy servers when it determines that the original server has failed, as well as application-management operations like deploying, updating, reimaging and scaling out applications. Dividing the datacenter into clusters isolates faults at the FC level, preventing certain classes of errors from affecting servers beyond the cluster in which they occur. FCs that serve a particular Azure cluster are grouped into FC Clusters.

FC Managed Operating Systems

An Azure OS base image Virtual Hard Disk (VHD) is deployed on all Host, Native, and Guest VMs in the Azure production environment. The three types of FC managed OS images are:

1. **Host OS:** Host OS is a customized version of the Windows OS that runs on Host Machine Root VMs

2. **Native OS:** Native OS runs on Azure native tenants such as the FC itself, Azure Storage and Load Balancer that do not have any hypervisor
3. **Guest OS:** Guest OS runs on Guest VMs (for IaaS, FC will run customer provided images on a VHD)

The Host OS and Native OS are OS images that run on physical servers and native tenants and host the Fabric Agent and other Host components. The Guest OS provides the most up-to-date runtime environment for Azure customers and can be automatically upgraded with new OS releases or manually upgraded based on customer preference.

Software Development Kits

Azure allows customers to create applications in many development languages. Microsoft provides language-specific Software Development Kits (SDKs) for .NET, Java, PHP, Ruby, Node.js and others. In addition, there is a general Azure SDK that provides basic support for any language, such as C++ or Python. These SDKs can be used with development tools such as Visual Studio and Eclipse.

These SDKs also support creating applications running outside the cloud that use Azure services. For example, a customer can build an application running on a Host that relies on Azure Blob Storage, or create a tool that automatically deploys Azure applications through the platform’s management interface.

Azure Services and Offerings

Azure services and offerings are grouped into categories discussed below. A complete list of Azure services and offerings available to customers is provided in the Azure Service Directory. Brief descriptions for each of the customer-facing services and offerings in scope for this report are provided below. Customers should consult extensive online documentation for additional information.

Compute

Azure App Service: Azure App Service enables customers to quickly build, deploy, and scale enterprise-grade web, mobile, and applications and programming interface (API) apps that can run on a number of different platforms.

- Azure App Service: API Apps: API Apps enables customers to build and consume Cloud APIs. Customers can connect their preferred version control system to their API Apps, and automatically deploy commits, making code changes.
- Azure App Service: App Center: App Center allows customers to accelerate mobile application development by providing a turnkey way to structure storage, authenticate users, and send push notifications. Mobile Apps allows customers to build connected applications for any platform and deliver a consistent experience across devices.
- Azure App Service: Web Apps: Web Apps offers secure and flexible development, deployment and scaling options for web applications of any size. Web Apps enables provisioning a production web application in minutes using a variety of methods including the Azure Portal, PowerShell scripts running on Windows, Command Line Interface tools running on any OS, source code control driven deployments, as well as from within the Visual Studio Integrated Development Environment (IDE).
- Azure App Service Static Web Apps: Static Web Apps offers streamlined full-stack development from source code to global high availability. It allows customers accelerated app development with a static front end and dynamic back end powered by serverless APIs. Customers experience high productivity with a tailored local development experience, GitHub native workflows to build and deploy apps, and unified hosting and management in the cloud.

Azure Arc: Azure Arc allows customers to manage, monitor and govern machines running on-premises or in other clouds, from Azure.

Azure Cloud Services: Azure Cloud Services is a PaaS service designed to support applications that are scalable, reliable, and inexpensive to operate. Azure Cloud Services is hosted on virtual machines. However, customers have more control over the VMs. Customers can install their own software on VMs that use Azure Cloud Services and access them remotely. It removes the need to manage server infrastructure and lets customers build, deploy, and manage modern applications with web and worker roles.

Azure Cloud Services (Extended Support): Azure Cloud Services (extended support) is a new Azure Resource Manager (ARM) based deployment model for Azure Cloud Services product. It has the primary benefit of providing regional resiliency along with feature parity with Azure Cloud Services deployed using Azure Service Manager. It also offers some ARM capabilities such as role-based access and control (RBAC), tags, policy, and supports deployment of ARM templates.

Azure Functions: Azure Functions is a serverless compute service that lets customers run event-triggered code without having to explicitly provision or manage infrastructure. Azure Functions is an event driven, compute-on-demand experience. Customers can leverage Azure Functions to build Hypertext Transfer Protocol (HTTP) endpoints accessible by mobile and Internet of Things (IoT) devices.

Azure Large Instances: Azure Large Instances is intended for critical workloads that require special architecture, certified hardware, or extraordinarily large servers. Azure Large Instances implementations are dedicated only to the customer, and customers have full access (root access) to the operating system (OS). Customers can manage OS and application installation according to their needs. For security, the instances are provisioned within the customer Azure Virtual Network (VNet) with no Internet connectivity.

Azure Machine Configuration: Azure Machine Configuration provides management and configuration capabilities to Azure compute resources in Azure and Arc VMs. Azure Machine Configuration uses the Azure policy to audit the internal configuration of a VM's OS, deployed applications, and the environment configuration. Azure Machine Configuration is a digital security and risk engineering DevOps Kit baseline control and helps audit VM configurations.

Azure Service Fabric: Azure Service Fabric is a distributed systems platform that makes it easy to package, deploy, and manage scalable and reliable microservices and containers. It is a micro-services platform used to build scalable managed applications for the cloud. Azure Service Fabric addresses significant challenges in developing and managing cloud applications by allowing developers and administrators to shift focus from infrastructure maintenance to implementation of mission-critical, demanding workloads.

Azure Virtual Desktop: Azure Virtual Desktop is a virtualization management service running on Azure that provisions and manages connections to virtual desktops and apps on Windows 7, Windows 10, Windows Server 2012 R2+ in single or multi-session environments. It allows users to set up a scalable and flexible environment as well as connect, deploy to, and manage virtual desktops.

Azure Virtual Machines: Azure Virtual Machines is one of the several types of on-demand, scalable computing resources that Azure offers. Virtual Machines, which includes Azure Reserved Virtual Machine Instances, lets customers deploy a Windows Server or a Linux image in the cloud. Customers can select images from a marketplace or use their own customized images. It gives customers the flexibility of virtualization without having to buy and maintain the physical hardware that runs it.

Azure Virtual Machine Scale Sets: Azure Virtual Machine Scale Sets service lets customers create and manage a group of identical, load balanced, and autoscaling VMs. It makes it possible to build highly scalable applications by allowing customers to deploy and manage identical VMs as a set. VM Scale sets are built on the Azure Resource Manager deployment model, are fully integrated with Azure load balancing and autoscaling, and support Windows and / or Linux custom images, and extensions.

Azure VM Image Builder: Azure VM Image Builder is an Azure Resource Provider service that allows customers to create custom virtual machine images.

Azure VMware Solution: Azure VMware Solution delivers a comprehensive VMware environment in Azure allowing customers to run native VMware workloads on Azure. Azure VMware Solution allows customers to seamlessly run, manage and secure applications across VMware environments and Microsoft Azure with a common operating framework.

Batch: Batch runs large-scale parallel applications and High-Performance Computing (HPC) workloads efficiently in the cloud. It allows customers to schedule compute-intensive tasks and dynamically adjust resources for their solution without managing the infrastructure. Customers can use Batch to scale out parallel workloads, manage the execution of tasks in a queue, and cloud-enable applications to offload compute jobs to the cloud.

Planned Maintenance: Planned Maintenance is responsible for the roll out of planned maintenance activities to the nodes and VMs in Azure.

Virtual Machines Licenses: Virtual Machines Licenses Offering provides customers with the necessary licenses for Windows Server and other software to run efficiently on Azure Virtual Machines. Virtual Machines Licenses ensure that customers have access to properly licensed software, enabling seamless and compliant operations within their virtual environments.

Containers

Azure Arc Enabled Kubernetes: Azure Arc Enabled Kubernetes allows customers (cluster operators) to use Azure as their single control plane for connecting, configuring and governing their Kubernetes clusters spread out across other public clouds and on-premise environments.

Azure Container Apps: Azure Container Apps is a fully managed environment that enables customers to run microservices and containerized applications on a serverless platform. Common uses of Azure Container Apps include deploying API endpoints, hosting background processing applications, handling event-driven processing, and running microservices.

Azure Container Instances: Azure Container Instances enables the creation of containers as first-class objects in Azure, without requiring VM management and without enforcing any prescriptive application model. Azure Container Instances is a solution for any scenario that can operate in isolated containers, without orchestration. Customer can run event-driven applications, quickly deploy from their container development pipelines, and run data processing and build jobs.

Azure Container Registry: Azure Container Registry allows customers the ability to store images for all types of container deployments including DC / OS, Docker Swarm, Kubernetes, and Azure services such as Azure App Service, Batch, Azure Service Fabric, and others. Developers can manage the configuration of apps isolated from the configuration of the hosting environment. Azure Container Registry reduces network latency and eliminates ingress / egress charges by keeping Docker registries in the same datacenters as customers' deployments. It provides local, network-close storage of container images within subscriptions, and full control over access and image names.

Azure Kubernetes Configuration Management: Azure Kubernetes Configuration Management allows customers (cluster operators) to use GitOps to manage configuration on various Kubernetes clusters - Azure Arc connected clusters, AKS clusters, and eventually other cluster types like Azure Red Hat OpenShift (ARO).

Azure Kubernetes Service (AKS): Azure Kubernetes Service is an enterprise ready managed service that allows customers to run Open source Kubernetes on Azure without having to manage it on their own. It also includes the functionality of Azure Container service (ACS), which was retired in calendar year Q1 2020. ACS was a container hosting environment which provided users the choice of container orchestration platforms such as Mesosphere DC/OS and Docker Swarm. AKS makes deploying and managing containerized applications easy. It offers serverless Kubernetes, an integrated continuous integration and continuous delivery (CI/CD) experience, and enterprise-grade security and governance. AKS unites the customer development and operations teams on a single platform to rapidly build, deliver, and scale applications with confidence.

Azure Red Hat OpenShift: Azure Red Hat OpenShift offering provides flexible, self-service deployment of fully managed OpenShift clusters. It helps customers maintain regulatory compliance and focus on their application development, while the master, infrastructure, and application nodes are patched, updated, and monitored by both Microsoft and Red Hat.

Microsoft Artifact Registry: Microsoft Artifact Registry is a registry of Docker and Open Container Initiative (OCI) images, with support for all OCI artifacts. It allows users to build, store, secure, scan, replicate, and manage container images and artifacts with a fully managed, geo-replicated instance of OCI distribution.

Networking

Application Gateway: Application Gateway is a web traffic load balancer that enables customers to manage traffic to their web applications. It is an Azure-managed layer-7 solution providing HTTP load balancing, Web Application Firewall (WAF), Transport Layer Security (TLS) termination service, and session-based cookie affinity to Internet-facing or internal web applications.

Azure Bastion: Azure Bastion is a managed PaaS service that provides secure and seamless Remote Desktop Protocol (RDP) and Secure Shell (SSH) access to customer's virtual machines directly through the Azure Portal. Azure Bastion is provisioned directly in the customer Virtual Network (VNet) and supports all VMs in their VNet using SSL without any exposure through public IP addresses.

Azure Communications Gateway: Azure Communications Gateway is a managed, cloud-based voice gateway that simplifies connecting operator fixed and mobile voice networks to Teams Phone. It combines a high-availability, Teams-certified and mobile-standards-compliant Session Border Controller (SBC) with API mediation function, removing the need for disruptive voice network changes and substantial IT system integration projects.

Azure Content Delivery Network: Azure Content Delivery Network (CDN) sends audio, video, applications, images, and other files faster and more reliably to customers by using the servers that are closest to each user. This dramatically increases speed and availability. Due to its distributed global scale, CDN can handle sudden traffic spikes and heavy loads without new infrastructure costs or capacity worries. CDN is built on a highly scalable, reverse-proxy architecture with sophisticated DDoS identification and mitigation technologies. Customers can choose to use Azure CDN from Verizon or Akamai partners. Verizon and Akamai are not covered in this SOC report.

Azure DDoS Protection: Azure DDoS Protection is a fully automated solution aimed primarily at protecting resources against Distributed Denial of Service (DDoS) attacks. Azure DDoS Protection helps prevent service interruptions by eliminating harmful volumetric traffic flows.

Azure DNS: Azure DNS is a hosting service for Domain Name System (DNS) domains that provides name resolution by using Microsoft Azure infrastructure. Azure DNS lets customers host their DNS domains alongside their Azure apps and manage DNS records by using the same credentials, APIs, tools, and billing as their other Azure services.

Azure ExpressRoute: Azure ExpressRoute lets customers create private connections between Azure datacenters and customer's infrastructure located on-premises or in a colocation environment. ExpressRoute connections do not go over the public Internet, and offer more reliability, faster speeds, and lower latencies than typical Internet connections.

Azure Firewall: Azure Firewall is a managed cloud-based network security service that protects Azure virtual network resources. It is a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability. Customers can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks. Azure Firewall uses a static public IP address for virtual network resources allowing outside firewalls to identify traffic originating from a virtual network. This service is fully integrated with Azure Monitor Essentials for logging and analytics purposes.

Azure Firewall Manager: Azure Firewall Manager is a security management service that provides central security policy and route management for cloud-based security perimeters. Azure Firewall Manager simplifies central configuration and management of rules for multiple Azure Firewall instances, across Azure regions and subscriptions. This allows customers to automate Azure Firewall deployment to multiple secured virtual hubs and integrates with trusted security partner solutions for advanced services.

Azure Front Door: Azure Front Door (AFD) is Microsoft's highly available and scalable Web Application Acceleration Platform, Global HTTP Load Balancer, Application Protection and Azure Content Delivery Network. AFD enables customers to build, operate and scale out their dynamic web application and static content. AFD provides customers' application with end-user performance, unified regional / stamp maintenance automation, Business Continuity and Disaster Recovery (BCDR) automation, unified client / user information, caching and service insights.

Azure Load Balancer: Azure Load Balancer distributes Internet and private network traffic among healthy service instances in cloud services or virtual machines. It lets customers achieve greater reliability and seamlessly add more capacity to their applications.

Azure NAT Gateway: Azure NAT (network address translation) Gateway simplifies outbound-only Internet connectivity for virtual networks. When configured on a subnet, all outbound connectivity uses specified static public IP addresses. Outbound connectivity is possible without a load balancer or public IP addresses directly attached to virtual machines.

Azure Network Function Manager: Azure Network Function Manager offers consistent Azure management experience for deploying network functions such as mobile packet core, SD-WAN edge, and VPN services on Azure Stack Edge devices. It simplifies governance and management by integrating with Azure tools and SDKs, enabling rapid deployment and improved network performance.

Azure Orbital Ground Station: Azure Orbital Ground Station is a fully managed end-to-end service that enables customers to communicate, downlink, and process data from their satellites' spacecrafts on a pay-as-you-go basis without needing them to build their own satellite ground stations.

Azure Peering Service: Azure Peering Service is a networking service that enhances customer connectivity to Microsoft cloud services such as Microsoft 365, Dynamics 365, SaaS services, Azure, or any Microsoft services accessible via the public Internet. Microsoft has partnered with Internet Service Providers (ISPs), Internet Exchange Partners, and Software-Defined Cloud Interconnect (SDCI) providers worldwide to provide reliable and high-performing public connectivity with optimal routing from the customer to the Microsoft network.

Azure Private Link: Azure Private Link provides private connectivity from a virtual network to Azure PaaS, customer-owned, or Microsoft partner services. It simplifies the network architecture and secures the connection between endpoints in Azure by eliminating data exposure to the public Internet.

Azure Private MEC: Azure Private MEC is a solution that delivers ultra-low-latency networking, applications, and services at the enterprise edge. It enables customers to accelerate time to market, reduce integration complexity, and improve security of end-to-end solutions.

Azure Route Server: Azure Route Server enables the customer's network appliances to exchange route information with Azure virtual networks dynamically. It allows customers to exchange routing information directly through Border Gateway Protocol (BGP) routing protocol between any Network Virtual Appliances (NVA) that supports the BGP routing protocol and the Azure Software Defined Network (SDN) in the Azure Virtual Network (VNET) without the need to manually configure or maintain route tables.

Azure Traffic Collector: Azure Traffic Collector enables sampling of network flows sent over the customer's ExpressRoute circuits. Flow logs get sent to a Log Analytics workspace where customers can create their own log queries for further analysis.

Azure Virtual Network: Azure Virtual Network lets customers create private networks in the cloud with full control over IP addresses, DNS servers, security rules, and traffic flows. Customers can securely connect a virtual network to on-premises networks by using a Virtual Private Network (VPN) tunnel, or connect privately by using the Azure ExpressRoute service.

Azure Virtual Network IP Services: Azure Virtual Network IP Services allows Internet resources to communicate inbound to Azure resources, as well as providing a predictable method for communicating outbound to the Internet and other public-facing Azure services. Customers can associate IP Services addresses to virtual machine network interfaces, public load balancers, VPN gateways, and other resources.

Azure Virtual Network Manager: Azure Virtual Network Manager is a management service that enables customers to group, configure, deploy, and manage virtual networks globally across subscriptions. With Virtual Network Manager, customers can define network groups to identify and logically segment their virtual networks. Customers can determine the connectivity and security configurations they want and apply them across all the selected virtual networks in network groups at once.

Azure Web Application Firewall: Azure Web Application Firewall helps protect customer's web apps from malicious attacks and top 10 Open Web Application Security Project (OWASP) security vulnerabilities, such as SQL injection and cross-site scripting. Cloud-native Azure Web Application Firewall service deploys in minutes and offers customized rules that meet the customer's web app security requirements.

Network Watcher: Network Watcher enables customers to monitor and diagnose conditions at a network scenario level. Network diagnostic and visualization tools available with Network Watcher allow customers to take packet captures on a VM, help them understand if an IP flow is allowed or denied on their Virtual Machine, find where their packet will be routed from a VM and gain insights to their network topology.

Traffic Manager: Traffic Manager is a DNS-based traffic load balancer that enables customers to distribute traffic optimally to services across global Azure regions, while providing high availability and responsiveness. Traffic Manager uses DNS to direct client requests to the most appropriate service endpoint based on a traffic-routing method and the health of the endpoints.

Virtual WAN: Virtual WAN is a networking service that brings many networking, security and routing functionalities together to provide a single operational interface. This service enables customers to automate large-scale branch connectivity which unifies network and policy management by optimizing routing using Microsoft global network.

VPN Gateway: VPN Gateway lets customers establish secure, cross-premises connections between their virtual network within Azure and on-premises IT infrastructure. VPN gateway sends encrypted traffic between Azure virtual networks over the Microsoft network. The connectivity offered by VPN Gateway is secure and uses the industry-standard protocols Internet Protocol Security (IPsec) and Internet Key Exchange (IKE).

Storage

Azure Archive Storage: Azure Archive Storage offers low-cost, durable, and highly available secure cloud storage optimized to store rarely accessed data that is stored for at least 180 days with flexible latency requirements (of the order of hours).

Azure Backup: Azure Backup protects Windows client data and shared files and folders on customer's corporate devices. Additionally, it protects Microsoft SharePoint, Exchange, SQL Server, Hyper-V virtual machines, and other applications in the customer's datacenter(s) integrated with System Center Data Protection Manager. Azure Backup enables customers to protect important data off-site with automated backup to Microsoft Azure.

Customers can manage their cloud backups from the tools in Windows Server, Windows Server Essentials, or System Center Data Protection Manager. These tools allow the user to configure, monitor and recover backups to either a local disk or Azure Storage.

Azure Data Box: Azure Data Box offers offline data transfer devices which are shipped between the customer's datacenter(s) and Azure, with little to no impact to the network. Azure Data Boxes use standard network-attached storage (NAS) protocols (Server Message Block (SMB)/CIFs and NFS), AES encryption to protect data, and perform a post-upload sanitization process to ensure that all data is wiped clean from the device. The data movement can be one-time, periodic, or an initial bulk data transfer followed by periodic transfers.

Azure Data Lake Storage Gen1: Azure Data Lake Storage (Gen1) provides a single repository where customers can capture data of any size, type, and speed without forcing changes to their application as the data scales. In the store, data can be shared for collaboration with enterprise-grade security. It is also designed for high-performance processing and analytics from Hadoop Distributed File System (HDFS) applications (e.g., Azure HDInsight, Data Lake Analytics, Hortonworks, Cloudera, MapR) and tools, including support for low latency workloads. For example, data can be ingested in real-time from sensors and devices for IoT solutions, or from online shopping websites into the store without the restriction of fixed limits on account or file size.

Azure File Sync: Azure File Sync is used to centralize file shares in Azure Files, while keeping the flexibility, performance, and compatibility of an on-premises file server. Azure File Sync transforms Windows Server into a quick cache of any Azure file share.

Azure Files: Azure Files offers fully managed file shares in the cloud that are accessible via the industry standard Server Message Block (SMB) protocol, Network File System (NFS) protocol, and Azure Files REST API. Azure file shares can be mounted concurrently by cloud or on-premises deployments. SMB Azure file shares are accessible from Windows, Linux, and macOS clients. NFS Azure file shares are accessible from Linux clients. Additionally, SMB Azure file shares can be cached on Windows servers with Azure File Sync for fast access near where the data is being used.

Azure HPC Cache: Azure HPC Cache is a file cache that speeds access to data for HPC tasks by caching files in Azure. It brings the scalability of cloud computing to existing workflows while allowing large datasets to remain in existing NAS or in Azure Blob storage.

Azure Managed Lustre: Azure Managed Lustre is a managed, pay-as-you-go file system for high-performance computing (HPC) and AI workloads that provides the open-source Lustre file system as a service. The Lustre file system is used in AI and HPC [High Performance Computing] scenarios for high-throughput applications.

Azure NetApp Files: Azure NetApp Files enables enterprise line-of-business and storage professionals to migrate and run complex, file-based applications with no code change. It is widely used as the underlying shared file-storage service in various scenarios. These include migration (lift and shift) of POSIX-compliant Linux and Windows applications, SAP HANA, databases, HPC infrastructure and apps, and enterprise web applications.

Azure Site Recovery: Azure Site Recovery contributes to a customer's BCDR strategy by orchestrating replication of their servers running on-premises or on Azure. The on-premises physical servers and virtual machine servers can be replicated to Azure or to a secondary datacenter. The virtual machine servers running in any Azure region can also be replicated to a different Azure region. When a disaster occurs in the customer's primary location, customers can coordinate failover and recovery to the secondary location using Azure Site Recovery and ensure that applications / workloads continue to run in the secondary location. Customers can failback their workloads to the primary location when it resumes operations. It supports protection and recovery of heterogeneous workloads (including System Center managed / unmanaged Hyper-V workloads, VMware workloads). With Azure Site Recovery, customers can use a single dashboard to manage and monitor their deployment and also configure recovery plans with multiple machines to ensure that machines hosting tiered applications failover in the appropriate sequence.

Azure Storage: Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. The Storage access control model allows each subscription to create one or more Storage accounts. Each Storage account has a primary and secondary secret key that is used to control access to the data within the Storage account. Every Storage service account has redundant data copies for fault tolerance. Listed below are the different storage types supported by Azure Storage:

- Blobs (including Data Lake Storage Gen2): Blobs is Microsoft's object storage solution for the cloud. Blobs can be used to store large amounts of binary data. For example, Blob Storage can be used for an application to store video, or to backup data. Azure Data Lake Storage Gen2 (a feature of Blobs) provides a hierarchical namespace, per object Access Control List (ACLs), and HDFS APIs.
- Data Lake Storage Gen2: Data Lake Storage Gen2 is a highly scalable and cost-effective data lake solution for Big Data analytics. It combines the power of a high-performance file system with massive scale and economy to help accelerate time to insight. Data Lake Storage Gen2 extends Azure Blob Storage capabilities and is optimized for analytics workloads and compliant file system interfaces with no programming changes or data copying.
- Disks: A managed or an unmanaged disk is a VHD that is attached to a VM to store application and system data. This allows for a highly durable and available solution while still being simple and scalable.
- Queues: Queues is a service for storing large number of messages. Queues provide storage and delivery of messages between one or more applications and roles.
- Tables: Tables provide fast access to large amounts of structured data that do not require complex SQL queries. For example, Tables can be used to create a customer contact application that stores customer profile information and high volumes of user transaction.
- Azure Disk Storage: Azure Disk Storage offers high throughput, high Input / Output Operations Per Second, and consistent low latency disk storage for Azure IaaS virtual machines. It allows the ability to dynamically change the performance of the SSD along with a customer's workloads without the need to restart VMs. Azure Disk Storage is suited for data-intensive workloads such as SAP HANA, top tier databases, and transaction-heavy workloads.
- Cool Storage: Cool Storage is a low-cost storage tier for cooler data, where the data is not accessed often. Example use cases for Cool Storage include backups, media content, scientific data, compliance and archival data. Customers can use Cool Storage to retain data that is seldom accessed.
- Premium Storage: Premium Storage delivers high-performance and low-latency storage support for virtual machines with input / output (IO) intensive workloads. Premium Storage is designed for mission-critical production applications.

Azure Storage Mover: Azure Storage Mover is a fully managed, hybrid migration service that enables customers to migrate on-premises file shares to Azure.

Databases

Azure Cache for Redis: Azure Cache for Redis gives customers access to a secure, dedicated cache for their Azure applications. Based on the open source Redis server, the service allows quick access to frequently requested data. Azure Cache for Redis handles the management aspects of the cache instances, providing customers with replication of data, failover, and Secure Socket Layer (SSL) support for connecting to the cache.

Azure Cosmos DB: Azure Cosmos DB was built from the ground up with global distribution and horizontal scale at its core. It offers turnkey global distribution across any number of Azure regions by transparently scaling and replicating customers' data wherever their users are. Customers can elastically scale throughput and storage worldwide, and pay only for the throughput and storage they need. Azure Cosmos DB guarantees single-digit-millisecond latencies at the 99th percentile anywhere in the world, offers multiple well-defined consistency models to fine-tune performance, and guarantees high availability with multi-homing capabilities - all backed by industry-leading, comprehensive SLAs.

Azure Database for MariaDB: Azure Database for MariaDB is a relational database based on the open-source MariaDB Server engine. It is a fully managed database as a service offering that can handle mission-critical workloads with predictable performance and dynamic scalability.

Azure Database for MySQL: Azure Database for MySQL is a relational database and a fully managed service built on Microsoft's scalable cloud infrastructure for application developers. Its built-in features maximize performance, availability, and security. Azure Database for MySQL empowers developers to focus on application innovation instead of database management tasks.

Azure Database for PostgreSQL: Azure Database for PostgreSQL is a relational database and a fully managed service built on Microsoft's scalable cloud infrastructure for application developers. Its built-in features maximize performance, availability, and security. Azure Database for PostgreSQL empowers developers to focus on application innovation instead of database management tasks.

Azure Database Migration Service: Azure Database Migration Service helps customers assess and migrate their databases and solve their compatibility and migration issues. The service is designed as a seamless, end-to-end solution for moving on-premises databases to the cloud.

Azure Health Data Services: Azure Health Data Services is an API for clinical health data that enables customers to create new systems of engagement for analytics, machine learning, and actionable intelligence with health data. Azure Health Data Services improves health technologies' interoperability and makes it easier to manage data.

Azure SQL: Azure SQL is a relational database service that lets customers rapidly create, extend, and scale relational applications into the cloud. Azure SQL delivers mission-critical capabilities including predictable performance, scalability with no downtime, business continuity, and data protection - all with near-zero administration. Customers can focus on rapid application development and accelerating time to market, rather than on managing VMs and infrastructure. Because the service is based on the SQL Server engine, Azure SQL provides a familiar programming model based on T-SQL and supports existing SQL Server tools, libraries and APIs.

Azure SQL Managed Instance: Azure SQL Managed Instance is a PaaS service that has near 100% compatibility with the latest Enterprise Edition SQL Server database engine, providing a native virtual network (VNet) implementation that addresses common security concerns, and a business model favorable to existing SQL Server customers. SQL Managed Instance allows existing SQL Server customers to lift and shift their on-premises applications to the cloud with minimal application and database changes.

Azure Synapse Analytics: Azure Synapse Analytics, formerly known as SQL Data Warehouse, is a limitless analytics service that brings together enterprise data warehousing and Big Data analytics. It lets customers scale data, either on-premises or in the cloud. Azure Synapse Analytics lets customers use their existing T-SQL knowledge to integrate queries across structured and unstructured data. It integrates with Microsoft data platform tools, including Azure HDInsight, Machine Learning Studio, Azure Data Factory, and Microsoft Power BI for a complete data-warehousing and business-intelligence solution in the cloud.

Microsoft Azure Managed Instance for Apache Cassandra: Microsoft Azure Managed Instance for Apache Cassandra provides automated deployment and scaling operations for managed open-source Apache Cassandra datacenters, accelerating hybrid scenarios and reducing ongoing maintenance.

SQL Managed Instance enabled by Azure Arc: SQL Managed Instance enabled by Azure Arc is designed to provide the existing SQL server applications an option to migrate to the latest version of the SQL Server engine and gain the PaaS style built in management capabilities without moving outside of the existing infrastructure, allowing customers to maintain the data sovereignty and meet other compliance criteria. This is achieved by leveraging the Kubernetes platform with Azure data services, which can be deployed on any infrastructure.

SQL Server enabled by Azure Arc: SQL Server enabled by Azure Arc extends Azure services to SQL Server instances hosted outside of Azure, in the customer's data center, in edge site locations like retail stores, or any public cloud or hosting provider. Azure Arc enables customers to manage all of their SQL Servers from a single point of control. As customers connect their SQL Servers to Azure, they get a single place to view the detailed inventory of their SQL Servers and databases.

SQL Server on Azure Virtual Machines: SQL Server on Azure Virtual Machines is a cloud database that allows users to migrate their SQL Server workloads to the cloud without having to manage any on-premise hardware. It can get the performance, security, and analytics of SQL Server backed by the flexibility and hybrid connectivity of Azure.

SQL Server Stretch Database: SQL Server Stretch Database helps customers migrate warm and cold transactional data transparently and securely to Azure while still providing inexpensive long data retention times.

Developer Tools

Azure App Configuration: Azure App Configuration allows customers to manage configuration within the cloud. Customers can create App Configuration stores to store key-value settings and consume stored settings from within applications, deployment pipelines, release processes, microservices, and other Azure resources. App Configuration allows customers to store and manage configurations effectively and reliably, in real time, without affecting customers by avoiding time-consuming redeployments.

Azure Deployment Environments: Azure Deployment Environments empowers development teams to quickly and easily spin up app infrastructure with project-based templates that establish consistency and best practices while maximizing security. This on-demand access to secure environments accelerates the stages of the software development lifecycle in a compliant and cost-efficient way.

Azure DevTest Labs: Azure DevTest Labs helps developers and testers quickly create environments in Azure while minimizing waste and controlling cost. Azure DevTest Labs creates labs consisting of pre-configured bases or Azure Resource Manager templates allowing customers to test the latest version of their application.

Azure for Education: Azure for Education provides resources for students to learn about programming, cloud technologies, and world-class developer tools.

Azure Lab Services: Azure Lab Services streamlines and simplifies setting up and managing resources and environments in the cloud. Azure Lab Services can quickly provision Windows and Linux virtual machines, Azure PaaS services, or complex environments in labs through reusable custom templates.

Azure Load Testing: Azure Load Testing is a fully managed load-testing service that enables customers to generate high-scale load. The service simulates traffic for applications, regardless of where they are hosted. Developers, testers, and quality assurance (QA) engineers can use it to optimize application performance, scalability, or capacity.

Azure Managed Grafana: Azure Managed Grafana is a fully managed service for analytics and monitoring solutions. It is supported by Grafana Enterprise, which provides extensible data visualizations. Grafana dashboards are deployed with built-in high availability and control access with Azure security.

Microsoft Dev Box: Microsoft Dev Box is an Azure service that gives developers self-service access to preconfigured, project-specific developer boxes. It provides developers the ability to connect on demand and work across multiple dev boxes to avoid configuration conflicts. Users can manage dev boxes with physical devices in Microsoft Intune to maximize security, compliance, and cost efficiency.

Service Connector: Service Connector is an Azure-managed service that helps developers easily connect compute services to target backing services. Service Connector configures the network settings and connection information between compute services and target backing services in the management plane.

Analytics

Azure Analysis Services: Azure Analysis Services, based on the proven analytics engine in SQL Server Analysis Services, is an enterprise grade Online analytical processing engine and BI modeling platform, offered as a fully managed PaaS service. Azure Analysis Services enables developers and BI professionals to create BI semantic models that can power highly interactive and rich analytical experiences in BI tools and custom applications.

Azure Chaos Studio: Azure Chaos Studio helps customers to measure, understand, and build application and service resilience to real-world incidents, such as a region going down or an application failure causing 100% CPU usage on a VM. With Chaos Studio, customers can run chaos engineering experiments that inject faults against their service and then monitor how the service responds to disruptions.

Azure Data Explorer: Azure Data Explorer is a fast and highly scalable, fully managed data analytics service for real-time analysis on large volumes of data streaming from applications, websites, IoT devices and more. Azure Data Explorer makes it simple to ingest this data and enables customers to quickly perform complex ad hoc queries on the data.

Azure Data Factory: Azure Data Factory is a fully managed, serverless data integration service that refines raw data at cloud scale into actionable business insights. Customers can construct Extract, Transform, Load processes code free in an intuitive visual environment, and easily operationalize and manage the data pipelines at scale.

Azure Data Share: Azure Data Share is a simple and safe service for sharing data, in any format and any size, from multiple sources with other organizations. Customers can control what they share, who receives the data, and the terms of use via a user-friendly interface.

Azure HDInsight: Azure HDInsight is a managed Apache Hadoop ecosystem offering in the cloud. It handles various amounts of data, scaling from terabytes to petabytes on demand, and can process unstructured or semi-structured data from web clickstreams, social media, server logs, devices, sensors, and more. Azure HDInsight includes Apache Hbase, a columnar NoSQL database that runs on top of the HDFS. This supports large transactional processing (Online Transaction Processing) of non-relational data, enabling use cases like interactive websites or having sensor data written to Azure Blob Storage. Azure HDInsight also includes Apache Storm, an open-source stream analytics platform that can process real-time events at large-scale. This allows processing of millions of events as they are generated, enabling use cases like IoT and gaining insights from connected devices or web-triggered events. Furthermore, Azure HDInsight includes Apache Spark, an open-source project in the Apache ecosystem that can run large-scale data analytics applications in memory. Lastly, Azure HDInsight incorporates R Server for Hadoop, a scale-out implementation of one of the most popular programming languages for statistical computing and machine learning. Azure HDInsight offers Linux clusters when deploying Big Data workloads into Azure.

Azure Operator Insights: Azure Operator Insights is a fully managed service that enables users with the collection and analysis of massive quantities of network data gathered from complex multi-part or multi-vendor network functions. It delivers statistical, machine learning, and AI-based insights for operator-specific workloads to help operators understand the health of their networks and the quality of their subscribers’ experiences in near real-time.

Azure Stream Analytics: Azure Stream Analytics is an event-processing engine that helps customers gain insights from devices, sensors, cloud infrastructure, and existing data properties in real-time. Azure Stream Analytics is integrated out of the box with Event Hubs, and the combined solution can ingest millions of events and do analytics to help customers better understand patterns, power a dashboard, detect anomalies, or kick off an action while data is being streamed in real time. It can apply time-sensitive computations on real-time streams of data by providing a range of operators covering simple filters to complex correlations, and combining streams with historic records or reference data to derive business insights quickly.

Data Catalog: Data Catalog is a fully managed service that serves as a system of registration and system of discovery for enterprise data sources. It lets users - from analysts to data scientists to developers - register, discover, understand, and consume data sources. Customers can use crowdsourced annotations and metadata to capture tribal knowledge within their organization, shine light on hidden data, and get more value from their enterprise data sources.

Data Lake Analytics: Data Lake Analytics is a distributed analytics service built on Apache Yet Another Resource Negotiator that scales dynamically so customers can focus on their business goals and not on distributed infrastructure. Instead of deploying, configuring and tuning hardware, customers can write queries to transform data and extract valuable insights. The analytics service can handle jobs of any scale instantly by simply setting the dial for how much power is needed. Customers only pay for their job when it is running, making the service cost-effective. The analytics service supports Microsoft Entra ID letting customers manage access and roles, integrated with on-premises identity system. It also includes U-SQL, a language that unifies the benefits of SQL with the expressive power of user code. U-SQL's scalable distributed runtime enables customers to efficiently analyze data in the store and across SQL Servers on Azure VMs, Azure SQL, and Azure Synapse Analytics.

Healthcare data solutions in Microsoft Fabric: Healthcare data solutions in Microsoft Fabric help healthcare organizations transform unstructured and semi-structured data into a suitable format for analysis, enabling exploratory analysis, large-scale analytics, and generative AI. These solutions break down data silos, harmonize disparate data, and provide real-time, data-driven insights to improve patient outcomes and drive innovation.

Microsoft Fabric: Microsoft Fabric is an all-in-one analytics solution for enterprises that covers everything from data movement to data science, real-time analytics, and business intelligence. Microsoft Fabric brings together new and existing components from Power BI, Azure Synapse, and Azure Data Factory into a single integrated environment. These components are then presented in various customized user experiences.

Power BI Embedded: Power BI Embedded is a service which simplifies how customers use Power BI capabilities with embedded analytics. Power BI Embedded simplifies Power BI capabilities by helping customers quickly add visuals, reports, and dashboards to their apps, similar to the way apps built on Microsoft Azure use services like Machine Learning and IoT. Customers can make quick, informed decisions in context through easy-to-navigate data exploration in their apps.

AI + Machine Learning

AI Builder: AI Builder is integrated with Power Platform and Power Automate capabilities that help customers improve business performance by automating processes and predicting outcomes. AI Builder is a turnkey solution that brings the power of AI through a point-and-click experience. With AI Builder, customers can add intelligence to their applications with little to no coding or data science experience.

Azure AI Foundry Portal: Azure AI Foundry provides a unified platform for enterprise AI operations, model builders, and application development. This foundation combines production-grade infrastructure with friendly interfaces, ensuring organizations can build and operate AI applications with confidence. Note: Only the Azure AI Foundry Portal is in-scope for this report.

Azure AI Services: Azure AI Services is the platform on which an evolving portfolio of REST APIs and SDKs enables developers to easily add intelligent services into their solutions to leverage the power of Microsoft's natural data understanding.

Azure AI Services: AI Anomaly Detector: Azure AI Services: AI Anomaly Detector enables customers to monitor and detect abnormalities in time series data with machine learning. It utilizes an API which adapts by automatically identifying and applying the best-fitting models to data, regardless of industry, scenario, or data volume. Using time series data, the API determines boundaries for anomaly detection, expected values, and which data points are anomalies.

Azure AI Services: Azure AI Containers: Azure AI services: Azure AI Containers provide several Docker containers that let customers use the same APIs that are available in Azure, on-premises. Using these containers gives customers the flexibility to bring Azure AI services closer to their data for compliance, security or other operational reasons.

Azure AI Services: Azure AI Content Safety: Azure AI Services: Azure AI Content Safety is a suite of intelligent screening tools that enhance the safety of customer's platform. Image, text, and video moderation can be configured to support policy requirements by alerting customers to potential issues such as pornography, racism, profanity, violence, and more.

Azure AI Services: Azure AI Custom Vision: Azure AI Services: Azure AI Custom Vision is an Azure AI Service that can train and deploy image classifiers and object detectors. The custom models trained by the AI service infer the contents of images based on visual characteristics.

Azure AI Services: Azure AI Document Intelligence: Azure AI Services: Azure AI Document Intelligence is an Azure AI Service that uses machine learning technology to identify and extract text, key / value pairs and table data from form documents. It ingests text from forms and outputs structured data that includes the relationships in the original file. Customers receive accurate results that are tailored to specific content without heavy manual intervention or extensive data science expertise. Azure AI Document Intelligence is comprised of custom models, the prebuilt receipt model, and the layout API. Customers can call Azure AI Document Intelligence models by using a REST API to reduce complexity and integrate it into a workflow or an application.

Azure AI Services: Azure AI Face Service: Azure AI Services: Azure AI Face Service is a service that has two main functions - face detection with attributes and face recognition. It provides the ability to detect human faces and compare similar ones, organize people into groups according to visual similarity, and identify previously tagged people in images.

Azure AI Services: Azure AI Immersive Reader: Azure AI Services: Azure AI Immersive Reader is a service that lets customers embed text reading and comprehension capabilities into applications. Azure AI Immersive Reader helps users of any age and reading ability with features like reading aloud, translating languages, and focusing attention through highlighting and other design elements.

Azure AI Services: Azure AI Language: Azure AI Services: Azure AI Language is a cloud-based service that provides Natural Language Processing (NLP) features for understanding and analyzing text. This service is used to help build intelligent applications using the web-based Language Studio, REST APIs, and client libraries. Azure AI Language includes language customization capabilities such as custom Named Entity Recognition (NER), custom text classification, and conversational language understanding.

Azure AI Services: Azure AI Metrics Advisor: Azure AI Services: Azure AI Metrics Advisor uses AI to perform data monitoring and anomaly detection in time series data. The service automates the process of applying models to the customer's data, and provides a set of APIs and a web-based workspace for data ingestion, anomaly detection, and diagnostics, without needing to know machine learning.

Azure AI Services: Azure AI Personalizer: Azure AI Services: Azure AI Personalizer offers customers automatic model optimization based on reinforcement learning through a cloud-based API service that helps client applications choose the best, single content item to show each user. Azure AI Personalizer collects and uses real-time information customers provide about content and context in order to select the most relevant content. Azure AI Personalizer uses system monitoring of customer and user behavior to report a reward score in order to improve its ability to select the best content based on the context information it receives. Content collected consists of any unit of information such as text, images, URLs, emails, and more.

Azure AI Services: Azure AI Search: Azure AI Services: Azure AI Search is a search as a service cloud solution that provides developers with APIs and tools for adding a rich search experience over customers' data in web, mobile, and enterprise applications.

Azure AI Services: Azure AI Speech: Azure AI Services: Azure AI Speech is an Azure service that offers speech to text, text to speech and speech translation using base (out of the box) and custom models.

Azure AI Services: Azure AI Translator: Azure AI Services: Azure AI Translator is a cloud-based machine translation service, translating natural language text between more than 60 languages, via a REST-based web service API. Besides translation, the API provides functions for dictionary lookup, language detection and sentence breaking.

Azure AI Services: Azure AI Video Indexer: Azure AI Services: Azure AI Video Indexer is a cloud application built as a cognitive video indexing platform that processes the videos that users upload and creates a cognitive index of the content within the video. It enables customers to extract the insights from videos using Video Indexer models.

Azure AI Services: Azure AI Vision: Azure AI Services: Azure AI Vision provides services to accurately identify and analyze content within images and videos. It also provides customers the ability to extract rich information from images to categorize and process visual data - and protect users from unwanted content.

Azure AI Services: Conversational Language Understanding: Azure AI Services: Conversational Language Understanding is a cloud-based API service that enables developers to build their custom language models (i.e., intent classifier and entity extractor). It enables its customers to integrate those custom machine-learning models into any conversational application, or unstructured text to predict, and pull out relevant, detailed information presented in a structured format i.e., JSON.

Azure AI Services: Question Answering: Azure AI Services: Question Answering is an Azure AI Services offering deployed on Azure. The endpoint is used by third party developers to create knowledge base endpoints. It allows users to distill information into an easy-to-navigate FAQ.

Azure AI Bot Service: Azure AI Bot Service helps developers build bots / intelligent agents and connect them to the communication channels their users are in. Azure AI Bot Service solution provides a live service (connectivity switch), along with SDK documentation, solution templates, samples, and a directory of bots created by developers.

Azure Health Bot: Azure Health Bot is an intelligent, highly personalized virtual health assistant that aims to improve the conversation between healthcare providers, payers and patients, via conversational navigation. It allows healthcare providers and payers to empower their users to get information related to their health, such as checking their symptoms, asking about their health plans, and receiving personalized, meaningful, credible answers, in an easy, self-serve and conversational way.

Azure Open Datasets: Azure Open Datasets service offers customers curated public datasets that can be used to add scenario-specific features to machine learning solutions for more accurate models. Azure Open Datasets are integrated into Azure Machine Learning and readily available to Azure Databricks and Machine Learning Studio (classic). Customers can also access the datasets through APIs and use them in other products, such as Power BI and Azure Data Factory. It includes public-domain data for weather, census, holidays, public safety, and location that helps customers train machine learning models and enrich predictive solutions.

Azure OpenAI Service: Azure OpenAI Service provides REST API access to OpenAI's language models including the GPT-3, Codex and Embeddings model series. These models can be adapted to the customer's specific task including content generation, summarization, semantic search, and natural language to code translation. Customers can access the service through REST APIs, Python SDK, or our web-based interface in the Azure OpenAI Studio.

Azure Machine Learning: Azure Machine Learning (ML) is a cloud service that allows data scientists and developers to prepare data, train, and deploy machine learning models. It improves productivity and lowers costs through capabilities such as automated ML, autoscaling compute, hosted notebooks and ML Ops. It is open-source friendly and works with any Python framework, such as PyTorch, TensorFlow, or scikit-learn.

Copilot for Service: Microsoft Copilot for Service is an AI assistant designed to enhance customer service experience and service representative productivity by integrating generative AI into existing contact centers. It seamlessly integrates with Microsoft apps like Outlook and Teams, as well as CRM solutions, providing real-time, data-driven insights from various content sources, including third-party knowledge bases.

Machine Learning Studio (Classic): Machine Learning Studio (Classic) is a service that enables users to experiment with their data, develop and train a model using training data and operationalize the trained model as a web service that can be called for predictive analytics.

Microsoft 365 Copilot for Sales: Microsoft 365 Copilot for Sales is a tool designed to increase productivity through CRM task automation, auto-generated email or meeting summaries, and more. Microsoft Copilot for Sales also generates AI-assisted content and recommendations, in addition to real-time customer opportunity insights.

Microsoft Genomics: Microsoft Genomics offers a cloud implementation of the Burrows-Wheeler Aligner and the Genome Analysis Toolkit for secondary analysis which are then used for genome alignment and variant calling.

Seeing AI: Seeing AI is a free consumer mobile app that narrates the world by using AI and describes nearby people, text, and objects for the blind and low vision community.

Internet of Things

Azure Digital Twins: Azure Digital Twins is an IoT platform that enables the customer's business to create a digital representation of real-world things, places, business processes, and people.

Azure Event Grid: Azure Event Grid is a high scale Pub / Sub service which enables event-driven programming. It integrates with webhooks for delivering events.

Azure IoT Central: Azure IoT Central is a managed IoT SaaS solution that makes it easy to connect, monitor, and manage IoT assets at scale.

Azure IoT Hub: Azure IoT Hub is used to connect, monitor, and control billions of IoT assets running on a broad set of operating systems and protocols. Azure IoT Hub establishes reliable, bi-directional communication with assets, even if they are intermittently connected, and analyzes and acts on incoming telemetry data. Customers can enhance the security of their IoT solutions by using per-device authentication to communicate with devices that have the appropriate credentials. Customers can also revoke access rights to specific devices to maintain the integrity of their system.

Azure Sphere: Azure Sphere is a secured, high-level application platform with built-in communication and security features for Internet-connected devices. It comprises a secured, connected, crossover microcontroller unit, a custom high-level Linux-based OS, and a cloud-based security service that provides continuous, renewable security.

Azure Time Series Insights: Azure Time Series Insights is used to collect, process, store, analyze, and query highly contextualized, time-series-optimized IoT-scale data. Time Series Insights is ideal for ad hoc data exploration and operational analysis. It is a uniquely extensible and customized service offering that meets the broad needs of industrial IoT deployments.

Device Update for IoT Hub: Device Update for IoT Hub enables customers to deploy over-the-air updates for IoT devices. It is an end-to-end platform that customers can use to publish, distribute, and manage over the air updates for all devices from tiny sensors to gateway level devices.

Event Hubs: Event Hubs is a Big Data streaming platform and event ingestion service capable of receiving and processing millions of events per second. Event Hubs can process, and store events, data, or telemetry produced by distributed software and devices. Data sent to an event hub can be transformed and stored by using any real-time analytics provider or batching / storage adapters. Event Hubs for Apache Kafka enables native Kafka clients, tools, and applications such as Mirror Maker, Apache Flink, and Akka Streams to work seamlessly with Event Hubs with only configuration changes. Event Hubs uses Advanced Message Queuing Protocol (AMQP), HTTP, and Kafka as its primary protocols.

Microsoft Cloud for Sustainability: Microsoft Cloud for Sustainability enables customers to reach their environmental sustainability goals and advance their conservation efforts with secure, globally scalable, and innovative IoT solutions. Customers can reduce their energy usage in their factory or building, monitor the quality of their water output and decrease material waste spillage, and also to help prevent wildlife poaching and keep watch on endangered habitats.

Microsoft Defender for IoT: Microsoft Defender for IoT provides customers with security protection by delivering unified visibility and control, adaptive threat prevention, and intelligent threat detection and response across IoT devices, IoT edges and IoT hubs running on-premises and in Azure cloud. It provides unified security management that enables end-to-end threat detection and analysis across hybrid cloud workloads and on customer’s Azure IoT solution.

Notification Hubs: Notification Hubs is a massively scalable mobile push notification engine for sending notifications to Android, iOS, and Windows devices. It aggregates sending notifications through the Apple Push Notification service, Firebase Cloud Messaging service, Windows Push Notification Service, Microsoft Push Notification Service, and more. It allows customers to tailor notifications to specific customers or entire audiences with just a few lines of code and do it across any platform.

Integration

API Management: API Management lets customers publish APIs to developers, partners, and employees securely and at scale. API publishers can use the service to quickly create consistent and modern API gateways for existing backend services hosted anywhere.

Azure Data Manager for Energy: Azure Data Manager for Energy helps energy companies gain actionable insights, improve operational efficiency, and accelerate time to market on the enterprise-grade, cloud-based OSDU (Open Subsurface Data Universe) data platform service. It supports innovation with a flexible, open energy platform that customers can customize according on their needs.

Azure Logic Apps: Azure Logic Apps automates the access and use of data across clouds without writing code. Customers can connect apps, data, and devices anywhere-on-premises or in the cloud, with Azure’s large ecosystem of SaaS and cloud-based connectors that includes Salesforce, Microsoft 365, Twitter, Dropbox, Google services, and more.

Azure Service Bus: Azure Service Bus is a multi-tenant cloud messaging service that can be used to send information between applications and services. The asynchronous operations enable flexible, brokered messaging, along with structured first-in, first-out messaging, and publish / subscribe capabilities. Service Bus uses AMQP, Service Bus Messaging Protocol (SBMP), and HTTP as its primary protocols. Additionally, Azure Relay is a multi-tenant service offering that enables connectivity across network boundaries without normally required networking infrastructure.

Universal Print: Universal Print is a modern print solution that organizations can use to manage their print infrastructure through cloud services from Microsoft. This cloud-based print solution provides secure printing, and eliminates the need for an on-premises infrastructure.

Identity

Azure Active Directory B2C: Azure Active Directory B2C extends Microsoft Entra ID capabilities to manage consumer identities. Azure Active Directory B2C is a comprehensive identity management solution for consumer-facing applications that can be integrated into any platform, and accessed from any device.

Microsoft Entra Domain Services: Microsoft Entra Domain Services provides managed domain services such as domain join, group policy, LDAP, Kerberos / NTLM authentication that are fully compatible with Windows Server Active Directory (AD). Customers can consume these domain services without the need to deploy, manage, and patch domain controllers in the cloud. Microsoft Entra Domain Services integrates with the existing Microsoft Entra ID tenant, thus making it possible for users to log in using their corporate credentials.

Microsoft Entra ID: Microsoft Entra ID (formerly Azure Active Directory) provides identity management and access control for cloud applications. To simplify user access to cloud applications, customers can synchronize on-premises identities, and enable single sign-on. Microsoft Entra ID comes in three editions: Free, Basic, and Premium. Self-service credentials management is a feature of Microsoft Entra ID that allows Microsoft Entra ID tenant administrators to register for and subsequently reset their passwords without needing to contact Microsoft support. Microsoft Online Directory Services (MSODS) is also a feature of Microsoft Entra ID that provides the backend to support authentication and provisioning for Microsoft Entra ID.

Microsoft Entra Permissions Management: Microsoft Entra Permissions Management is a cloud infrastructure entitlement management (CIEM) service that provides comprehensive visibility and control over permissions for all identities and resources in customer's Microsoft Azure, Amazon Web Services (AWS) and Google Cloud Platform (GCP) accounts. It detects, automatically right-sizes, and continuously monitors for unused and excessive permissions.

Microsoft Global Secure Access: Microsoft Global Secure Access is designed to provide secure and seamless access to applications and resources, regardless of location. Built upon the core principles of Zero Trust, it ensures least privilege, explicit verification, and assumes breach to maintain security.

Microsoft Purview Information Protection: Microsoft Purview Information Protection controls and helps secure email, documents, and sensitive data that customers share outside their company walls. Microsoft Purview Information Protection provides enhanced data protection capabilities to customers and assists them with classification of data using labels and permissions. Microsoft Purview Information Protection includes Azure Rights Management, which used to be a standalone Azure service.

Management and Governance

Application Change Analysis: Application Change Analysis is a subscription-level Azure resource provider. It checks for resource changes in the subscription, and provides data for various diagnostic tools to help users understand what changes might have caused issues.

Automation: Automation lets customers create, deploy, monitor, and maintain resources in their Azure environment automatically by using a highly scalable and reliable workflow execution engine. Automation enables customers to create their PowerShell content (Runbooks) or choose from many available in the Runbook Gallery, and trigger job execution (scheduled or on-demand). Customers can also upload their own PowerShell modules and make use of them in their Runbooks. The distributed service takes care of executing the jobs per customer-specified schedule in a reliable manner, providing tenant context, tracking, and debugging as well as authoring experience.

Azure Advisor: Azure Advisor is a personalized recommendation engine that helps customers follow Azure best practices. It analyzes Azure resource configuration and usage telemetry, and then provides recommendations that can reduce costs and improve the performance, security, and reliability of applications.

Azure Blueprints: Azure Blueprints provides governed subscriptions to enterprise customers, simplifying largescale Azure deployments by packaging key environment artifacts, role-based access controls, and policies in a single blueprint definition.

Azure Lighthouse: Azure Lighthouse offers service providers a single control plane to view and manage Azure across all their customers with higher automation, scale, and enhanced governance. With Azure Lighthouse, service providers can deliver managed services using comprehensive and robust management tooling built into the Azure platform. This offering can also benefit enterprise IT organizations by managing resources across multiple tenants.

Azure Managed Applications: Azure Managed Applications enables customers to offer cloud solutions that are easy for consumers to deploy and operate. It can help customers implement the infrastructure and provide ongoing support. A managed application can be made available to all customers or only to users in the customer's organization by publishing it in the Azure marketplace or to an internal catalog, respectively.

Azure Migrate: Azure Migrate enables customers to migrate to Azure, also serving as a single point to track migrations to Azure. Customers can choose from Microsoft first-party and Independent Software Vendor (ISV) partner solutions for their assessment and migration activities. Customers can plan and carry out migration of their servers using the Server Assessment and Server Migration tools; these are Microsoft solutions available on Azure Migrate. Server Assessment helps to discover on-premise applications and servers (Hyper-V and VMware VMs), and provides a migration assessment: a mapping from discovered servers to recommended Azure VMs, migration readiness analysis and cost estimates to run the VMs in Azure. It allows for dependency visualization to view dependencies of a single VM or a group of VMs. Server Migration allows customers to migrate the on-premises servers (non-virtualized physical or virtualized using Hyper-V and VMware) to Azure. Microsoft solutions to assess and migrate database workloads - Database Assessment and Database Migration - are also discoverable on Azure Migrate. In addition to these tools, ISV partner tools for assessment and migration are also discoverable on Azure Migrate. The machines discovered using these tools and the assessment and migration activities conducted using these tools can be tracked on Azure Migrate; this helps customers to track all their migration activities at one place.

Azure Monitor: Azure Monitor provides full observability into a customer's applications, infrastructure and networks and collects, analyzes and acts on telemetry data from Azure and on-premises environments. It helps customers maximize performance and availability of applications and proactively identifies problems in real time. It includes, but is not limited to, the following four services: Azure Monitor Essentials, Application Insights, Application Insights Profiler, and Log Analytics.

- Azure Monitor Essentials: Azure Monitor Essentials is a centralized dashboard which provides detailed up-to-date performance and utilization data, access to the activity log that tracks every API call, and diagnostic logs that help customers debug issues in their Azure resources.
- Application Insights: Application Insights is used to monitor any connected App; It is on by default to be able to monitor multiple types of Azure resources, particularly Web Applications. It includes analytics tools to help diagnose issues and understand what users do with the App. It can monitor and analyze telemetry from mobile apps by integrating with Visual Studio App Center.
- Application Insights Profiler: Application Insights Profiler is used to help understand and troubleshoot performance issues in production. It helps teams collect performance data in a low-impact way to minimize overhead to the system.
- Log Analytics: Log Analytics enables customers to collect, correlate and visualize all their machine data, such as event logs, network logs, performance data, and more, from both on-premises and cloud assets. It enables transformation of machine data into near real-time operational intelligence for better decision making. Customers can search, correlate, or combine outputs of search from multiple data sources regardless of volume, format, or location. They can also visualize their data, separate signals from noise, with powerful log-management capabilities.

Azure Policy: Azure Policy provides real-time enforcement and compliance assessment on Azure resources to apply standards and guardrails.

Azure Quotas: Azure Quotas enables Azure end customers to view and manage quotas for Azure Services by subscription. It provides the capability to request Quota increase inline for adjustable quotas and eliminate latency between the fulfillment and what customer can see in their portal.

Azure Resource Graph: Azure Resource Graph is a service designed to extend Azure Resource Management by providing efficient and performant resource exploration with the ability to query at scale across a given set of subscriptions so that customers can effectively govern their environment. Azure Resource Graph offers the ability to query resources with complex filtering, grouping and sorting by resource properties and the ability to iteratively explore resources based on governance requirements. Resource Graph also offers the ability to assess the impact of applying policies in a vast cloud environment.

Azure Resource Manager (ARM): Azure Resource Manager (ARM) enables customers to repeatedly deploy their app and have confidence that their resources are deployed in a consistent state. Customers can define the infrastructure and dependencies for their app in a single declarative template. This template is flexible enough for use across all customer environments such as test, staging, or production. If customers create a solution from the Azure Marketplace, the solution will automatically include a template that customers can use for their app. With Azure Resource Manager, customers can put resources with a common lifecycle into a resource group that can be deployed or deleted in a single action. Customers can see which resources are linked by any dependencies. Moreover, they can control who in their organization can perform actions on the resources. Customers manage permissions by defining roles and adding users or groups to the roles. For critical resources, they can apply an explicit lock that prevents users from deleting or modifying the resource. ARM logs all user actions so customers can audit those actions. For each action, the audit log contains information about the user, time, events, and status.

Azure Resource Mover: Azure Resource Mover helps customers smoothly orchestrate moves for various Azure resources between regions. Customers can move resources to different Azure regions to align to a region launch, align for services / features, respond to business developments, align for proximity, meet data requirements, respond to deployment requirements or respond to decommissioning. Azure Resource Mover provides a single hub for moving resources across regions, allowing for reduced move time and complexity, simple and consistent experience, easy identification of dependencies, automatic cleanup of resources, and testing.

Azure Signup Portal: Azure Signup Portal enables customers to sign up for Azure subscriptions. The service handles pre-requisites for signup such as Commerce account creation, Payment Instrument attachment, agreement acceptance, etc., and then finally funnels the user down to provisioning of a new subscription.

Azure Update Manager: Azure Update Manager service helps manage updates for all customers machines, including those running on Windows and Linux, across Azure, on-premises, and on other cloud platforms. It helps customers with monitoring update compliance from a single dashboard, make system updates in real-time, schedule updates within a maintenance window, or automatically update during off-peak hours.

Cloud Shell: Cloud Shell provides a web-based command line experience from Ibiza portal, Azure mobile, docs.microsoft.com, shell.azure.com, and Visual Studio Code. Both Bash and PowerShell experiences are available for customers to choose from.

Cost Management: Cost management is an external offering for cloud cost management capabilities included with Azure subscriptions for financial governance for the customer’s organization. It provides the ability to explore cost and usage data via multidimensional analysis, where creating customized filters and expressions allow the customer to answer consumption-related questions for their Azure resources.

Microsoft Azure Portal: Microsoft Azure Portal provides a framework SDK, telemetry pipeline and infrastructure for Microsoft Azure services to be hosted inside the Azure Portal shell, and manages and monitors the required components to allow Azure services to run in a single, unified console. Azure is designed to abstract much of the infrastructure and complexity that typically underlies applications (i.e., servers, operating systems, and network) so that developers can focus on building and deploying applications. Microsoft Azure portal simplifies the development work for Azure service owners and developers by providing a comprehensive SDK with tools and controls for easily building and packaging the service applications. Customers manage these Azure applications through the Microsoft Azure Portal and Service Management API (SMAPI). Users who have access to Azure customer applications are authenticated based on their Microsoft Accounts (MSA) and / or Organizational Accounts. Azure customer billing is handled by MOCP. MOCP and MSA / Organizational Accounts and their associated authentication mechanisms are not in scope for this SOC report.

Microsoft Purview (Governance): Microsoft Purview (Governance) is a unified data governance service that helps customers manage and govern on-premises, multi-cloud, and SaaS data. Customers can easily create a holistic, up-to-date map of their data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Note: Only the Microsoft Purview Governance sub-offering is in-scope for this report.

Security

Azure Confidential Computing: Azure Confidential Computing offers customers with solutions to enable isolation of sensitive data while it is being processed in the cloud. Azure Confidential Computing lets processing of data from multiple sources without exposing the input data to other parties. This type of secure computation enables many scenarios like anti-money laundering, fraud-detection, and secure analysis of healthcare data.

Azure Confidential Ledger: Azure Confidential Ledger provides customers a managed and decentralized ledger for data entries backed by Blockchain. Customers can maintain data integrity by preventing unauthorized or accidental modification with tamperproof storage. The service helps protect customer’s data at rest, in transit, and in use with hardware-backed secure enclaves used in Azure Confidential Computing.

Azure Dedicated HSM: Azure Dedicated HSM provides cryptographic key storage in Azure where the customer has full administrative control over the Hardware Security Module (HSM). It offers a solution for customers who require the most stringent security requirements.

Azure Payment HSM: Azure Payment HSM is a bare metal Infrastructure as a Service (IaaS) that provides cryptographic key operations for real-time payment transactions in Azure. It is delivered using Thales payShield 10K payment HSMs and meets the most stringent payment card industry (PCI) requirements for security, compliance, low latency, and high performance.

Customer Lockbox for Microsoft Azure: Customer Lockbox for Microsoft Azure provides an interface for customers to review and approve or reject customer data access requests. It is used in cases where a Microsoft engineer needs to access customer data during a support request.

Key Vault: Key Vault safeguards keys and other secrets in the cloud by using HSMs. It protects cryptographic keys and small secrets like passwords with keys stored in HSMs. For added assurance, customers can import or generate keys in HSMs that are FIPS 140-2 Level 2 certified. Key Vault is designed so that Microsoft does not see or extract customer keys. Customers can create new keys for Dev-Test in minutes and migrate seamlessly to production keys managed by security operations. Key Vault scales to meet the demands of cloud applications without the need to provision, deploy, and manage HSMs and key management software.

Microsoft Azure Attestation: Microsoft Azure Attestation enables customers to verify the identity and security posture of a platform before the user interacts with it. Azure Attestation receives evidence from the platform, validates it with security standards, evaluates it against configurable policies, and produces an attestation token for claims-based applications. The service supports attestation of trusted platform modules (TPMs) and trusted execution environments (TEEs) and virtualization-based security (VBS) enclaves.

Microsoft Copilot for Security: Microsoft Copilot for Security empowers security and IT teams to protect organizations at the speed and scale of AI. It is a generative AI-powered security solution that helps increase the efficiency and capabilities of defenders to improve security outcomes at machine speed and scale. It helps support security professionals in end-to-end scenarios such as incident response, threat hunting, intelligence gathering, and posture management.

Microsoft Defender Experts for Hunting: Microsoft Defender Experts for Hunting is a proactive threat hunting service that goes beyond the endpoint to hunt across endpoints, Microsoft 365, cloud applications, and identity. Microsoft Defender Experts will investigate any findings and hand off the associated contextual alert information, along with remediation instructions, to customers so they can quickly respond.

Microsoft Defender Experts for XDR: Microsoft Defender Experts for XDR is a managed extended detection and response service that helps Security Operations Centers (SOCs) focus on and accurately respond to incidents that matter. It provides extended detection and response for customers who use the following Microsoft Defender XDR services: Microsoft Defender for Endpoint, Microsoft Defender for Microsoft 365, Microsoft Defender for Identity, Microsoft Defender for Cloud Apps, and Microsoft Entra ID.

Microsoft Defender for Cloud: Microsoft Defender for Cloud helps customers prevent, detect, and respond to threats with increased visibility into and control over the security of Azure resources. It provides integrated security monitoring and policy management across Azure subscriptions, helps detect threats that might otherwise go unnoticed, and works with a broad ecosystem of security solutions. Key capabilities include monitoring the security state of customer's Azure resources, policy-driven security maintenance, analysis of security data while applying advanced analytics, machine learning and behavioral analysis, prioritized security alerts as well as insights into the source of the attack and impacted resources.

Microsoft Defender Threat Intelligence: Microsoft Defender Threat Intelligence (Defender TI) is a platform that streamlines triage, incident response, threat hunting, vulnerability management, and cyber threat intelligence analyst workflows when conducting threat infrastructure analysis and gathering threat intelligence. Defender TI enables security professionals to focus on what actually helps their organization defend themselves, deriving insights about the actors through analysis and correlation instead of spending time on the data discovery, collection, and parsing of data.

Microsoft Sentinel: Microsoft Sentinel is a cloud-native Security Information and Event Management (SIEM) platform that uses built-in AI to help analyze large volumes of data across an enterprise. Microsoft Sentinel aggregates data from all sources, including users, applications, servers, and devices running on-premises or in any cloud, letting customers reason over millions of records in a few seconds. It includes built-in connectors for easy onboarding of security solutions.

Multi-Factor Authentication: Multi-Factor Authentication (MFA) helps prevent unauthorized access to on-premises and cloud applications by providing an additional layer of authentication. MFA follows organizational security and compliance standards while also addressing user demand for convenient access. MFA delivers strong authentication via a range of options, including mobile apps, phone calls, and text messages, allowing users to choose the method that works best for them.

Windows Autopatch: Windows Autopatch is a cloud service that automates Windows, Microsoft 365 Apps for Enterprise, Microsoft Edge, and Microsoft Teams updates to improve security and productivity across a customer's organization.

Media

Azure Media Services: Azure Media Services offers cloud-based versions of many existing technologies from the Microsoft Media Platform and Microsoft media partners, including ingest, encoding, format conversion, content protection and both on-demand and live streaming capabilities. Whether enhancing existing solutions or creating new workflows, customers can combine and manage Media Services to create custom workflows that fit every need.

Web

Azure Fluid Relay: Azure Fluid Relay is a managed offering for the Fluid Framework that helps developers build real-time collaborative experiences and replicate state across connected JavaScript clients in real-time. The Fluid Framework is a collection of client libraries for distributing and synchronizing shared state.

Azure Maps: Azure Maps is a collection of geospatial services and SDKs that use fresh mapping data to provide geographic context to web and mobile applications. Azure Maps enables features such as map drawing, routing, search, time zones and traffic. The APIs can be subscribed to by customers in the Azure Portal or ARM.

Azure SignalR Service: Azure SignalR service is a managed service to help customers easily build real-time applications with SignalR technology. This real-time functionality allows the service to push content updates to connected clients, such as a single page web or a mobile application. As a result, clients are updated without the need to poll the server or submit new HTTP requests for updates.

Azure Spring Apps: Azure Spring Apps service makes it easy to deploy Spring Boot-based microservice applications to Azure with zero code changes. It manages the infrastructure of Spring Cloud applications, so developers can focus on their code. It provides lifecycle management using comprehensive monitoring and diagnostics, configuration management, service discovery, CI/CD integration, blue-green deployments, and more.

Azure Web PubSub: The Azure Web PubSub service helps customers build real-time messaging web applications using WebSockets and the publish-subscribe pattern easily. This real-time functionality allows publishing content updates between server and connected clients (for example a single page web application or mobile application).

Mixed Reality

Remote Rendering: Remote Rendering enables customers to render high quality interactive 3D content in the cloud and stream it in real-time to devices running on the edge.

Spatial Anchors: Spatial Anchors helps customers create spatially aware mixed reality experiences across iOS, Android, and HoloLens devices. Customers can use this cross-platform service to unlock mixed reality capabilities like wayfinding, and enhance collaboration in facilities management, training, gaming, and other scenarios.

Hybrid + Multicloud

Azure Arc enabled System Center Virtual Machine Manager: Azure Arc enabled System Center Virtual Machine Manager allows on-premises System Center Virtual Machine Manager (SCVMM) customers to connect their SCVMM environment to Azure and perform VM self-service operations from the Azure portal. Additionally, customers can manage, monitor, and govern machines running on-premises from Azure through Arc.

Azure Arc enabled VMware vSphere: Azure Arc enabled VMware vSphere performs full lifecycle management on VMware VMs and uses Azure RBAC to provision and manage VMs on demand in the Azure portal. It performs access governance, monitoring, update management, and security at scale for VMware VMs from customer datacenters or by using Azure VMware Solution, Kubernetes clusters, and VMware Tanzu Application Service.

Azure Center for SAP Solutions: Azure Center for SAP solutions is an Azure offering that makes SAP a top-level workload on Azure. Azure Center for SAP solutions is an end-to-end solution that enables customers to create and run SAP systems as a unified workload on Azure and provides a more seamless foundation for innovation. Customers can take advantage of the management capabilities for both new and existing Azure-based SAP systems.

Azure Kubernetes Service on Azure Stack HCI: Azure Kubernetes on Azure Stack HCI (hyperconverged infrastructure) uses Azure Arc to create new Kubernetes clusters on Azure Stack HCI directly from Azure. It enables customers to use familiar tools like Azure portal, Azure CLI (Command Line Interface), and Azure Resource Manager templates to create and manage their Kubernetes clusters running on Azure Stack HCI. Since clusters are automatically connected to Arc when they are created, customers can use their Microsoft Entra ID for connecting to their clusters from anywhere. This ensures developers and application operators to provision and configure Kubernetes clusters in accordance with company policies.

Azure Operator Nexus: Azure Operator Nexus is a carrier-grade hybrid cloud platform built for mission-critical mobile network applications. It helps customers simplify provisioning of new network services, optimize deployment of network functions and applications on-premises, and run network-intensive workloads and mission-critical applications with resiliency, security, observability, and high performance.

Azure Operator Service Manager: Azure Operator Service Manager is a cloud orchestration service designed to simplify management of complex edge network services hosted on the Azure Operator Nexus platform. It provides customers with persona-based capabilities to onboard, compose, deploy and update multi-vendor applications across one-to-many Azure sites and regions.

Azure Monitor for SAP Solutions: Azure Monitor for SAP solutions is an Azure-native monitoring product that enables customers to monitor availability, performance, and operation of SAP systems running on Azure.

Internal Supporting Services

Internal Supporting Services is a collection of services that are not directly available to third-party customers. They are included in SOC examination scope for Azure and Azure Government because they are critical to platform operations or support dependencies by first-party services, e.g., Microsoft 365 and Dynamics 365.

Access Monitoring: Access Monitoring (AM) evaluates permissions throughout the infrastructure to report on effective access across Cloud + AI. AM drives reporting in the quarterly User Access Review and several KPIs inside the division.

AIP Masters: AIP Masters is a data processing pipeline that produces two business intelligence data sets (Azure Usage and Customer Catalog) used by other Azure services. The Azure Usage data set includes consumption data of Azure services by Azure customers at the subscription and meter level and the Customer Catalog dataset contains non-PII customer metadata and identifiers associated with Azure subscriptions.

Asimov Event Forwarder: Asimov Event Forwarder reads full event stream from OneDS Collector and breaks it apart into separate event streams based upon a set of subscription matching criteria. These event streams are then forwarded to the downstream services which subscribe to that stream.

Atlas: Atlas (formerly OneIdentity) is used for managing user accounts and security groups in different domains.

Autopilot Security: Autopilot Security manages major parts of the security of the Azure core control plane, such as Certificate management and rollover, as well as the management of encryption and decryption keys. These services are related to Autopilot and Pilotfish systems that the rest of the Azure stack depends on.

AzCP Platform: AzCP Platform is a set of Service Fabric (SF) applications that install a SF cluster with a declarative deployment model paired with a collection of microservices to fill in gaps in the out-of-the-box support for common application needs within the Azure Control Plane.

Azure Marketplace Portal: Azure Marketplace Portal is the new marketplace for Azure applications. It is an online store for thousands of certified, open source, and community software applications, developer services, and data pre-configured for Azure.

Azure Code Scanning: Azure Code Scanning offers anti-malware scanning service for Azure service teams and services to protect against malware. Azure Code Scanning uses multiple anti-malware scanning engines to detect malware and Potentially Unwanted Programs (PUP).

Azure Diagnostic Services: Azure Diagnostic Services helps Azure customers and Support engineers to troubleshoot customer issues and identify root cause and recovery actions.

Azure Notebooks Component: Azure Notebooks Component is an internal service that allows Microsoft teams to embed a component that provides a Jupyter notebook canvas allowing teams to add themes, languages, etc. to their applications.

Azure Security Monitoring (ASM SLAM): ASM SLAM contains the features and services related to Security Monitoring in Azure. This includes Azure Security Pack which is deployed by services to configure their security monitoring.

Azure Service Health: Azure Service Health is a suite of experiences that provide personalized guidance and support when issues in Azure services are affecting or may affect customers in the future.

Azure Service Manager (RDFE)[8]: Azure Service Manager (RDFE) is a communication path from the user to the Fabric used to manage Azure services. It represents the publicly exposed classic APIs, which is the frontend to the Azure Portal and the SMAPI. All requests from the user go through Azure Service Manager (RDFE) or the newer ARM.

Azure Stack Bridge: Azure Stack Bridge is an integration service which provides hybrid capabilities between on-premise Azure Stack deployments and the online Azure cloud.

Azure Stack Diagnostics and Analytics Service: Azure Stack Diagnostics and Analytics Service enables Azure Stack devices to upload telemetry and ingest the data into Kusto for edge observability.

Azure Stack Edge Service: Azure Stack Edge Service, formerly known as Data Box Edge Service, manages appliances on customer premises that ingest data to customer storage account over network.

Azure Stack Telemetry (Online)[13]: Azure Stack Telemetry (Online) is a service that collects and processes telemetry data from Azure Stack environments, including deployment statistics and operational information. This data helps monitor and improve customer experiences, security, application health, quality, and performance.

Azure Support Center: Azure Support Center provides tools for the internal technical support team to diagnose and resolve support requests from Azure customers.

Azure System Lockdown: Azure System Lockdown is a feature within Azure Security Pack which monitors and audits applications running on other services in the execution environment.

Azure Throttling Solutions: Azure Throttling Solutions builds standardized throttling solutions for Microsoft Cloud Services. It partners with the Azure office of the Chief Technology Officer (CTO) (AOCTO) to deliver throttling solutions that best serve first-party Microsoft rate-limiting needs.

Azure Usage Billing: Azure Usage Billing (AUB or Oro) is the central service which enables collection and processing of billing usage across Azure. It is an analytics service designed to help customers analyze and process streams of billing and usage data that can be used to get insights, build reports or trigger alerts and actions.

Azure Watson: Azure Watson is an internal tool for service troubleshooting and crash dump analysis.

[13] Examination period for this offering / service was from October 1, 2024, to March 31, 2025.

Blueshift Analytics: Blueshift Analytics is a Big Data service for internal Microsoft allowing them to run large scale batch jobs on data stored in Azure Data Lake Store Gen2.

Cloudfit: Cloudfit is a service that provides machine utilization analysis and recommendations to improve cost of goods sold (COGS) for all Microsoft services.

CloudMine: CloudMine is a data pipeline and data store for engineering artifacts such as work items, builds, commit, or source code. It serves data spanning multiple systems, organizations, and years of history in a single data store, allowing users to query engineering data across the Microsoft enterprise.

CO+IE-Hardware Inventory: Cloud Operations and Innovation Engineering (CO+IE) Hardware Inventory provides users with information on metadata of physical assets in Cloud Operations and Innovation (CO+I) data centers.

Copilot Applied AI: Copilot Applied AI (formerly Dynamics 365 Insights Apps AI and B360 AI Platform) provides internal AI services to products built by other teams within Dynamics 365 Insights Apps (formerly Business 360). The Dynamics 365 Insights Apps AI service leverages Microsoft data sources (Search Logs, Browser Logs) and other 1st and 3rd party data to enrich consumer profiles (B2C).

CoreWAN: CoreWAN is used to connect all Microsoft products worldwide to the Internet. It is composed of software, firmware, hardware devices, physical sites around the world, and terrestrial fiber optic cables, submarine fiber optic cables, and leased circuits from carriers.

CSCP-ReferenceSystems: CSCP Reference Systems enable the automation of capacity planning, management and execution with a set of data and services that are the "central source of truth" for Master Data with continuous validation of accuracy, freshness and completeness.

Datacenter Secrets Management Service (dSMS): dSMS is an Azure service that handles, stores, and manages the lifecycle for Azure Foundational Services.

Datacenter Security Token Service (dSTS): dSTS provides a highly available and scalable security token service for authenticating and authorizing clients (users and services) of Azure Foundation and Essential Services.

Datacenter Service Configuration Manager (dSCM): dSCM enables service teams to onboard to Azure Security internal services by providing specific configuration settings. The goal of dSCM is to reduce the onboarding and configuration management time for services onboarding to Azure Security services.

DataGrid: DataGrid system is comprised of a metadata repository system to store data contract for all Common Schema events and data ingested from SQL, Azure SQL, Azure Tables, Azure Queues, CSV and TSV files.

Dynamics 365 Integrator App: Dynamics 365 Integrator App is responsible for the sync of data between all Dynamics 365 platforms.

Dynamics 365 Office Integration: Dynamics 365 Office Integration is used to capture Document Management using SharePoint, OneDrive for Business document recommendations, and OneNote Export to Excel within Dynamics CRM.

Enterprise Data Platform: Enterprise Data Platform is a data pipeline service that collects, analyzes and shares back value add telemetry to Microsoft Enterprise customers.

Environmental Sustainability Green SKU - Data Platform: Environmental Sustainability Green SKU - Data Platform provides science-based calculations for carbon emission computation for the Emission Impact Dashboard and Carbon platform.

Exotic & Private Cloud - Resource Providers: Exotic & Private Cloud - Resource Providers is an Azure Specialized resource provider, billing and validation service focused on baremetal networking scenarios. The service builds on existing Azure infrastructure and Azure Networking stack to enable workloads with external partners into Azure Cloud.

ExP - Managed: ExP - Managed Service is an A/B testing platform which provides Microsoft teams with a tool to easily run A/B experiments.

ExP Treatment Assignment Service: ExP Treatment Assignment service provides HTTP REST endpoints for customers to retrieve configuration for A/B testing and exposure control. This includes variants (flights), feature flags (treatment variables), assignment context and the experimentation blob.

Fabric Controller Fundamental Services: Fabric Controller Fundamental Services, earlier known as Compute Manager, is an Azure core service responsible for the allocation of Azure tenants and their associated containers (VMs) to the hardware resources in the datacenter, and for the management of their lifecycle. Subcomponents include the Service Manager (SM / Aztec), Tenant Manager, Container Manager and Allocator.

Fabric Network Devices: Fabric Network Devices is used to provide all datacenter connectivity for Azure. Fabric Network Devices is completely transparent to Azure customers who cannot interact directly with any physical network device. The Fabric Network Devices service provides APIs to manage network devices in Azure datacenters. It is responsible for performing write operations to the network devices, including any operation that can change the code or configuration on the devices. The API exposed by Fabric Network Devices is used to perform certain operations, e.g., enable / disable a port for an unresponsive blade. It hosts all code and data necessary to manage network devices and does not have any dependency on services that are deployed after the build out.

Falcon: Falcon is a pseudo-serverless ecosystem that enables teams across Microsoft to build highly scalable microservices powering various features that span across Bing, Skype and Microsoft 365.

Gateway Manager: Gateway Manager is a control plane for VPN, ExpressRoute, Application Gateway, Azure Firewall, and Bastion. It is a critical component in Hybrid Azure Networking.

Geneva Actions: Geneva Actions is an extensible platform enabling compliant management of production services and resources running on the Azure Cloud. It allows users to plug in their own live site operations to the Geneva Actions authorization and auditing system to ensure safe and secure control of the Azure platform.

Geneva Analytics Orchestration: The Geneva Analytics Platform (Cloud Analytics Service) includes Data Studio, the Geneva Catalog, Geneva Job Scheduler, Geneva Collector and satellite micro-services. The Geneva Analytics Platform provides tools for Data Discovery, Data Transformations and Data Movement to internal Microsoft Teams. It integrates with other Azure Cloud Engineering Systems: The Geneva Pipeline, IcM, Geneva Health, etc.

Geneva Warm Path: Geneva Warm Path is a monitoring / diagnostic service used by teams across Microsoft to monitor the health of their service deployments.

Groups and Experimentation (OSG): Groups and Experimentation (OSG) Supports assignment of users and devices into groups for experimentation and targeting for scenarios such as OS build flighting, Storefront UX experiments, and DevCenter app Betas.

Holmes Service: Holmes service provides resource management and controls to trigger and influence actions on resources. Holmes is agnostic to specific types of service-model, & type of inventory, and tries to optimize packing, reshape clusters, apply required policies, and tools for various scenarios.

IcM Incident Management Service: IcM is a unified incident management system for all Microsoft services and provides tools for managing live site and on call rotations across the world.

Interflow: Interflow is a threat intelligence exchange service. It collects threat data (botnet IPs, hashes of malicious files, etc.) from various Microsoft teams and from various third parties, and then shares that data back out to Microsoft teams so they can act on it in their own products and services.

JIT: Just In Time (JIT) access provides engineers temporary elevated access to production services when needed to perform servicing activities and support their services.

LENS APLU: APLU (Account Profile Look Up) aims to improve CELA's response time to law enforcement requests. It consolidates the information gathering process and replaces multiple tools with a single efficient API. CELA users can use CRM to submit requests to APLU, which then retrieves information from various E+D services and the processed information is then delivered back to the CST Portal, streamlining the overall response process for CELA.

Lens Explorer: Lens Explorer is part of the Geneva Analytics offering. It allows users to quickly drill down into customer’s data and build dashboards that tell them a story.

M365D Automated IR: M365D Automated IR is a service that holds the logic for automated remediation of threats related to malicious or suspicious activity for customers using Microsoft Defender XDR (Extended Detection and Response).

M365D Investigation and Exploration: M365D Investigation and Exploration service is a web portal through which subscribers of M365D service can consume Threat Intelligence and the results of processed cyber event data including indications of attack, indications of compromise, etc.

M365D Management Service: M365D Management Service is a service which registers customers for the Microsoft Defender 365 service and allows them to onboard their organization’s machines.

MDM: MDM (Multi-Dimensional-Metrics) is the component within Geneva Monitoring responsible for collection and aggregation of metrics, performing alerting and visualizing health information.

MEE Privacy Service: MEE Privacy Service, also known as Next Generation Privacy Common Infrastructure, is a set of services that provides Data Subject Rights (DSR) distribution and auditing for internal Microsoft GDPR compliance. The service acts as the entry point for all view, export, delete and account close DSR signals that are then fanned out to various agents throughout the company to process in their data sets. Each of those agents then send back completion / acknowledgement signals that are subsequently used to produce several audit reports used to report Microsoft’s GDPR compliance to executive management.

Microsoft Bot Framework: Microsoft Bot Framework represents the offline tools, SDKs, CLIs, etc. that support the Azure AI Bot Service offering.

Microsoft Emissions Impact Dashboard: The Emissions Impact Dashboard helps Microsoft cloud customers understand, track, report, analyze, and reduce carbon emissions associated with their cloud usage.

Microsoft Email Orchestrator: Microsoft Email Orchestrator (formerly called Azure Email Orchestrator) is an internal service for managing email content and for sending email communications to customers across Microsoft.

MSaaS File Management (DTM V2): MSaaS File Management is required to exchange files between customers, CSS, and Agents.

MSFT.RR DNS: MSFT.RR DNS is the Microsoft internal Recursive DNS for internal consumption.

Network Billing: Network Billing service provides a reliable pipeline with low-latency for services in Azure Networking.

On-Premises Data Gateway: On-Premises Data Gateway provides connectivity to on-premises resources for Power BI, Power Apps, and LogicApps services.

OneBranch Release: OneBranch Release is the release manager for services to deploy to all clouds in a secure and compliant manner.

OneDeploy Deployment Infrastructure (DE): OneDeploy Development Infrastructure is an Azure Deployment Engine (DE) custom workflow execution for Azure Foundational / Core services.

OneDS Collector: OneDS Collector is the ingestion front end for the telemetry pipelines used by Microsoft Windows, Microsoft 365 and other Microsoft products. Microsoft products are instrumented with telemetry clients for logging and sending telemetry in the form of events. OneDS Collector validates and scrubs the events, then forwards them to the Asimov Event Forwarder service.

OneSettings: OneSettings service provides a command and control surface for numerous clients in the ecosystem. Primarily utilized to control the rate of Telemetry events collected by the Universal Telemetry Client (UTC) powering scenarios like Diagnostics, Experimentation and configuration.

PF-FC: PilotFish Fabric Controller (PF-FC) is the PilotFish hosted environment for managing the underlying hardware and services related to the Azure Fabric Controller. This includes buildout and management of the environments in PF, health of the nodes, FC role management and startup.

Pilotfish: Pilotfish is available to first-party customers (e.g., Microsoft 365, Dynamics 365) for the management of hyper-scale services used in high-availability scenarios. Customers are guaranteed a defined level of service health, health monitoring, reporting and alerting, secure communications between servers, secure Remote Desktop Protocol (RDP) capability, and full logical and physical machine lifecycle management.

PMI Foundation: PMI Foundation provides customers with a hardened, trusted platform that is standardized and scalable to support baremetal identity services.

Resource Provider Service as a Service: Resource Provider Service as a Service is a platform for Microsoft teams to develop their resource providers internally. It hosts first/third party resource providers such as Oracle.

Service Tree: Service Tree enables Microsoft employees to model organizations, software, and offerings as a single system of record with associated metadata and resources. This service maintains an auditable and up-to-date directory of software, processes, and metadata to enable security, compliance, reliability, and automation.

SIPS ML Detections 2: SIPS ML Detections 2 service analyzes Azure logs to detect potential attacks compromises, such as account compromise, data breach, web attacks, compromised hosts, against Azure and Azure customers.

SQL Business Analytics[14]**:** SQL Business Analytics is an internal tool that allows Azure SQL engineers to leverage service telemetry to aggregate data to generate reports identifying the usage, growth, and other business critical trends for Azure SQL and Open Source database (OSS database) products.

Unified Remote Scanning (URSA): Unified Remote Scanning (URSA) provides a unified and standardized platform for remote security scans across Azure.

[14] Examination period for this offering / service was from April 1, 2024, to September 30, 2024.

Vulnerability Scanning & Analytics: Vulnerability Scanning & Analytics is a service that provides vulnerability management and analytics for physical / virtual machines in cloud environments.

WaNetMon: WaNetMon monitors the health and availability of the Azure network and its services across all regions and all cloud environments. The platform provides monitoring, alerting and diagnostics capabilities for the Azure networking DRIs to quickly detect and diagnose issues. WaNetMon is also responsible for democratization of all network telemetry data, getting the data to a common data store and making it accessible for everyone.

Windows Azure Jumpbox: Windows Azure Jumpboxes are used by Azure service teams to operate Azure services. Jumpbox (hop-box) servers allow access to and from datacenters. They function as utility servers for runners, deployments, and debugging.

Workflow: Workflow lets users upload their workflows to Azure and have them executed in a highly scalable manner. This service is currently consumed only by Microsoft 365 SharePoint Online service.

Microsoft Online Services

Appsource: Appsource is an enterprise app marketplace which integrates with other major Microsoft platforms including Dynamics and Microsoft 365 to allow an easy click-try-buy process.

Dynamics 365 Customer Voice: Dynamics 365 Customer Voice is a simple yet comprehensive survey solution that builds on the current survey-creation experience of Microsoft Forms in Microsoft 365. It offers new capabilities that make capturing and analyzing customer and employee feedback simpler than ever. Customers can respond to the surveys by using any web browser or mobile device. As responses are submitted, Power BI reports can be used to analyze them and make decisions in real time.

Endpoint Attack Notifications: Endpoint Attack Notifications is a managed threat hunting service that provides Security Operation Centers (SOCs) with expert level monitoring and analysis to help them ensure that critical threats in their unique environments do not get missed.

Intelligent Recommendations: Intelligent Recommendations enables businesses to automate relevant recommendations, including personalized results for new and returning users, and the ability to interpret both user interactions and item or user metadata. In return, businesses receive tailored recommendations models based on their needs and business logic. Intelligent Recommendations frees companies from the tedious management of editorial collections. Instead, it helps drive engagement, run experiments, and build trust with consumers.

Microsoft Copilot Studio: Microsoft Copilot Studio is an offering that enables anyone to create powerful chatbots using a guided, no-code graphical interface, without the need for data scientists or developers. It eliminates the gap between subject matter experts and the development teams building the chatbots, and the long latency between subject matter experts recognizing an issue and updating a chatbot to address it. It removes the complexity of exposing teams to the nuances of conversational AI and the need to write complex code. It also minimizes the IT effort required to deploy and maintain a custom conversational solution by empowering subject matter experts and departments to build and maintain their own conversational solutions.

Microsoft Defender for Cloud Apps: Microsoft Defender for Cloud Apps is a comprehensive service that provides customers the ability to extend their on-premise controls to their cloud applications and provide deeper visibility, comprehensive controls, and improved protection for these apps. Microsoft Defender for Cloud Apps provides Shadow IT discovery, information protection to cloud applications, threat detection and in-session controls.

Microsoft Defender for Endpoint: Microsoft Defender for Endpoint is unified platform for preventative protection, post-breach detection, automated investigation, and response. Microsoft Defender for Endpoint protects endpoints from cyber threats, detects advanced attacks and data breaches, automates security incidents, and improves security posture.

Microsoft Defender for Identity: Microsoft Defender for Identity is a cloud-based security solution that leverages on-premises Active Directory (AD) signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at the organization.

Microsoft Graph: Microsoft Graph exposes multiple APIs from Microsoft 365 and other Microsoft cloud services through a single endpoint. Microsoft Graph simplifies queries that would otherwise be more complex. Customers can use Microsoft Graph and Microsoft Graph Webhooks to:

- Access data from multiple Microsoft cloud services, including Microsoft Entra ID, Exchange Online as part of Microsoft 365, SharePoint, OneDrive, OneNote, and Planner.
- Navigate between entities and relationships.
- Access intelligence and insights from the Microsoft cloud (for commercial users).

Microsoft Intune: Microsoft Intune provides mobile device management, mobile application management, and PC management capabilities from the cloud. Using Intune, organizations can provide their employees with access to corporate applications, data, and resources from virtually anywhere on almost any device, while helping to keep corporate information secure.

Microsoft Managed Desktop: Microsoft Managed Desktop combines Microsoft 365 Enterprise with an IT-as-a-Service backed by Microsoft, for providing the best user experience, the latest technology as well as Desktop security and IT services, with an end-to-end cloud-based solution that is managed, supported, and monitored by Microsoft.

Microsoft Stream: Microsoft Stream provides a common destination for video management, with built-in intelligence features, and the IT management and security capabilities that businesses of all sizes require. It is a fully managed SaaS service for enterprise customers in which users can upload, share and view videos within a small team, or across an entire organization, all inside a securely managed environment. Microsoft Stream leverages Azure AI services that enable in-video face detection and speech-to-text transcription that enhances learning and productivity. Microsoft Stream also includes IT admin capabilities for managing video content and increases engagement within an organization by integrating video into the applications used every day. Microsoft Stream utilizes built-in, industry-leading encryption and authenticated access to ensure videos are shared securely.

Nomination Portal: Nomination Portal is an optimized customer relation management solution for Azure On-boarding and Nomination to Engagement Customer Lifecycle. It provides increased transparency on Azure services offered and what the customer is taking to production, a clearer idea of where IPs are needed with improved assignment and activity redecoration, as well as capturing effort towards customer engagements.

PowerApps: PowerApps enables customers to connect to their existing systems and create new data, build apps without writing code, and publish and use the apps on the web and mobile devices. Services under PowerApps include, but are not limited to, the following:

- **PowerApps Authoring Service**: PowerApps Authoring Service is a component service that supports the PowerApps service for authoring cross-platform applications without the need to write code. It provides the service to visually compose the app using a browser, to connect to data using different connections and APIs, and to generate a packaged application that is published to the PowerApps Service. The packaged application can be previewed using the service while authoring or it can be shared and played on iOS, Android and Windows Phone.
- **PowerApps MakerX Portal**: PowerApps MakerX Portal is the management website for PowerApps, where users can sign up for the product and perform management operations on PowerApps and related resources. It communicates directly with the PowerApps Service RP for most operations and provides entry points for users to launch into other PowerApps services as necessary.

- **PowerApps Service RP**: PowerApps Service RP is the back-end RESTful service for PowerApps that handles the management operations for PowerApps and related entities such as connections and APIs. Architecturally, the resource provider (RP) is an ARM RP, meaning that incoming requests are authenticated by the ARM on the front end and proxied through to the RP.

Power Automate: Power Automate helps customers set up automated workflows between their favorite apps and services to synchronize files, get notifications, collect data, and more.

Power BI: Power BI is a suite of business analytics tools to analyze data and share insights. Power BI dashboards provide a 360-degree view for business users with their most important metrics in one place, updated in real time, and available on all of their devices. With one click, users can explore the data behind their dashboard using intuitive tools that make finding answers easy. Power BI facilitates creation of dashboards with over 50 connections to popular business applications and comes with pre-built dashboards crafted by experts that help customers get up and running quickly. Customers can access their data and reports from anywhere with the Power BI Mobile apps, which update automatically with any changes to customers data.

Windows Update for Business reports: Windows Update for Business reports is a cloud-based solution that provides information about the customer’s Microsoft Entra ID-joined devices' compliance with Windows updates. Windows Update for Business reports is offered through the Azure portal, and it's included as part of the Windows 10 or Windows 11 prerequisite licenses. Windows Update for Business reports helps customers monitor security, quality, driver, and feature updates for Windows 11 and Windows 10 devices, report on devices with update compliance issues, and analyze and display the customer’s data in multiple ways.

Microsoft Dynamics 365

Chat for Dynamics 365: Chat for Dynamics 365 is one of the primary channels for customers to interact with support agents because of its simplicity and ease of use. Customer service centers prefer customers to connect via Chat for Dynamics 365 because it allows service agents to be more productive by simultaneously engaging with multiple customers.

Dataverse: Dataverse securely stores and manages data that is used by business applications. Data within Dataverse is stored within a set of entities (An entity is a set of records used to store data, similar to how a table stores data within a database). Dataverse includes a base set of standard entities that cover typical scenarios, but also lets the customer create custom entities specific to their organization and populate them with data using Power Query. App makers can then use Power Apps to build rich applications using this data.

Dynamics 365 AI Customer Insights: Dynamics 365 AI Customer Insights is a cloud-based SaaS service that enables organizations of all sizes to bring together data from multiple sources and generate knowledge and insights to build a holistic 360 degree view of their customers.

Dynamics 365 Athena - CDS to Azure Data Lake: Export to Data Lake (Athena) is a pipeline to continuously export data from the Dataverse to Azure Data Lake Gen2. It is designed for enterprise big data analytics, is cost-effective, scalable, has high availability / disaster recover capabilities and enables best in class analytics performance. Data is stored in the Common Data Model format which provides semantic consistency across apps and deployments. The standardized metadata and self-describing data in an Azure Data Lake Gen2 facilitates metadata discovery and interoperability between data producers and consumers such as Power BI, Azure Data Factory, Azure Databricks, and Azure Machine Learning service.

Dynamics 365 Business Central: Dynamics 365 Business Central, formerly known as Dynamics NAV, is Microsoft’s Small and Medium Business service built on and for the Azure cloud. It provides organizations with a service that supports their unique requirements and rapidly adjusts to constantly changing business environments, without the additional overhead of managing infrastructure.

Dynamics 365 Commerce, Dynamics 365 Finance, and Dynamics 365 Supply Chain Management: These offerings are supported by the same set of underlying services. These offerings provide customers with a complete set of adaptable ERP functionality that includes financials, demand planning, procurement / supply chain, manufacturing, distribution, services industries, public sector and retail capabilities that are combined with BI, infrastructure, compute and database services.

Dynamics 365 Contact Center: Dynamics 365 Contact Center is a Copilot-first contact center solution that works with existing customer relationship management systems (CRMs). It supports contact centers by providing channels of communication, self-service functions, intelligent routing and agent-assisted services.

Dynamics 365 Customer Insights - Data: Dynamics 365 Customer Insights - Data (formerly Dynamics 365 Customer Insights Engagement insights) enables customers to understand interactively how their customers are using their services and products - both individually and holistically - on websites, mobile apps, and connected products. Customers can combine behavioral analytics with transactional, demographic, survey, and other data types from Dynamics 365 Customer Insights.

Dynamics 365 Customer Insights - Journeys: Dynamics 365 Customer Insights - Journeys (formerly Dynamics 365 Marketing) is a marketing-automation application that helps customers turn prospects into business relationships. Dynamics 365 Customer Insights - Journeys has built-in intelligence to allow customers to create emails and online content to support marketing initiatives, organize and publicize events, and share information.

Dynamics 365 Customer Service: Dynamics 365 Customer Service provides tools / apps that help build great customer relationships by focusing on optimum customer satisfaction. It provides many features and tools that organizations can use to manage the services they provide to customers.

Dynamics 365 Field Service: Dynamics 365 Field Service business application helps organizations deliver onsite service to customer locations. It combines workflow automation, algorithm scheduling, and mobility to help mobile workers fix issues when they are onsite at the customer location.

Dynamics 365 Fraud Protection: Dynamics 365 Fraud Protection provides customers with a payment fraud solution helping e-commerce merchants drive down fraud loss, increase bank acceptance rates to yield higher revenue, and improve the online shopping experience for its customers.

Dynamics 365 Guides: Dynamics 365 Guides is a mixed-reality application for Microsoft HoloLens that lets operators learn, during the flow of work by providing holographic instructions when and where they are needed. These instruction cards are visually tethered to the place where the work must be done, and can include images, videos, and 3D holographic models. Operators see what must be done, and where. Therefore, they can get the job done faster, with fewer errors and greater skill retention.

Dynamics 365 Human Resources: Dynamics 365 Human Resources provides a Microsoft-hosted HR solution that delivers core HR functionality to HR professionals, managers and employees across the organization.

Dynamics 365 Intelligent Order Management: Dynamics 365 Intelligent Order Management enables customers to manage the orchestration of orders through fulfillment helping organizations orchestrate order flows across different platforms and apps. Intelligent Order Management is designed to operate in complex environments where there are many internal and external systems and partners that enable the supply chain processes. The platform is designed to scale up and down with a business, regardless of the organization size.

Dynamics 365 Project Operations: Dynamics 365 Project Operations connects sales, resourcing, project management, and finance teams in a single application to win more deals, accelerate project delivery, and maximize profitability.

Dynamics 365 Remote Assist: Dynamics 365 Remote Assist enables customers to collaborate more efficiently by working together from different locations on HoloLens, HoloLens 2, Android, or iOS devices.

Dynamics 365 Resource Scheduling Optimization: Dynamics 365 Resource Scheduling Optimization is an Add-in for Dynamics 365 Field Service that automatically schedules jobs to the resources that are best equipped to complete them. For example, Resource Scheduling Optimization can schedule work orders for field technicians or cases for customer service reps. While the schedule board and the schedule assistant help schedule a single job, this add-in can schedule multiple jobs at once. It maximizes resource use and minimizes travel time.

Dynamics 365 Sales: Dynamics 365 Sales enables sales professionals to build strong relationships with their customers, take actions based on insights, and close sales faster. It can be used to keep track of customer accounts and contacts, nurture sales from lead to order, and create sales collateral.

Dynamics 365 Sales Insights: Dynamics 365 Sales Insights empowers sellers to deliver personalized engagement and build profitable relationships. Capabilities include supercharging sales with a prioritized list of everything that needs to be done and optimizing the sales cadence for different types of prospects with sequences.

Microsoft Power Platform on Azure: Microsoft Power Platform on Azure services are enabled in Dynamics 365 Relevance Search (RS) by default. Microsoft Power Platform on Azure provides additional backend features to improve Dynamics 365 Relevance Search. These features include natural language search with Intent understanding, knowledge-based query annotation, semantic parsing to create structured queries, spell checking, query rewriting to normalize synonyms and abbreviations, and world common knowledge to understand location, date, time, holiday, and popular organizations. Additional features include multi-level ranking and a customer feedback loop which consumes user clicks to train and improve the rankers.

Nuance Conversational IVR: Nuance Conversational IVR is a Microsoft first party multi-tenant SaaS platform that provides an enterprise-grade robust interactive voice response (IVR) service. It integrates with telephony and contact center systems to provide callers natural, human-like self-service interactions and advanced IVR capabilities by utilizing the latest Microsoft and Nuance Conversational AI technologies.

Power Pages: Power Pages is a secure, enterprise-grade, low-code software as a service (SaaS) platform for creating, hosting, and administering modern external-facing business websites. Power Pages empowers customers to rapidly design, configure, and publish websites that work across web browsers and devices.

Additionally, Dynamics 365 Life Cycle Services and Power Platform Admin Center are underlying features across multiple Dynamics 365 offerings. Dynamics 365 Life Cycle Services is a collaboration portal that provides an environment and a set of regularly updated services that can help customers manage the application lifecycle of their implementations of finance and operations apps. The Power Platform Admin Center provides a unified portal for administrators to manage environments and settings for Power Apps, Power Automate, and customer engagement apps.

Microsoft Cloud for Financial Services

Microsoft Cloud for Financial Services: Microsoft Cloud for Financial Services provides capabilities to manage data to deliver differentiated experiences, empower employees, and combat financial crime. It also facilitates security, compliance, and interoperability. This set of cloud-based solutions enhances collaboration, automation, and insights to streamline processes; personalizes every customer interaction; improves customer experience; and delivers rich data insights. The data model enables Microsoft’s partners and customers to extend the value of the platform with additional solutions to address the financial industry’s most urgent challenges. These capabilities will help organizations align to business and operational needs, and then deploy quickly to accelerate time to value. Microsoft Cloud for Financial Services and its capabilities (Unified Customer Profile, Customer Onboarding, and Collaboration Manager) are built atop Azure, Microsoft Dynamics 365, Microsoft Power Platform, and Microsoft 365 offerings. Microsoft 365 related offerings are not in the scope of this examination.

Unified Customer Profile: Unified Customer Profile helps banks tailor their customer experiences via a 360-degree view of the customer and, bringing together financial, behavioral, and demographic data.

Customer Onboarding: Customer Onboarding provides customers with easy access loan apps and self-service tools, helping to streamline the loan process to enhance customer experience and loyalty while increasing organizational and employee productivity. Helps customers efficiently apply for and keep track of a loan by streamlining the application process. Additionally, it empowers loan officers to manage loan applications with workflow automation, streamlining and customizing operations to meet specific lending needs.

Collaboration Manager: Collaboration Manager helps banks bring collaboration seamlessly into their lending workflows enabling them to improve process orchestration from front office to back office and facilitate omnichannel communications with customers. This capability helps banks improve organization and employee productivity, unlock value creation, and enhance customer experience. The portions of this capability covered by Microsoft 365 are not in scope for this examination.

Description of Controls

Security Organization - Information Security Program

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

The objective of the Information Security Program is to maintain the Confidentiality, Integrity, and Availability 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 environment, develop mitigating strategies and implement security controls, define roles and responsibilities (including qualification requirements), coordination of different corporate departments and implement security controls based on corporate, legal and regulatory requirements. In addition, team specific Standard Operating Procedures (SOPs) are developed and approved annually by appropriate management to provide implementation details for carrying out specific operational tasks in the following areas:

1. Access Control
2. Anti-Malware
3. Asset Management
4. Baseline Configuration
5. Business Continuity and Disaster Recovery
6. Capacity Management
7. Cryptographic Controls
8. Datacenter Operations
9. Document and Records Management
10. Exception Process
11. Hardware Change and Release Management
12. Incident Management
13. Legal and Regulatory Compliance
14. Logging and Monitoring
15. Network Security

16. Penetration Testing
17. Personnel Screening
18. Privacy
19. Risk Management
20. Security Development Lifecycle
21. Software Change and Release Management
22. Third Party Management
23. Training and Awareness
24. Vulnerability Scanning and Patch Management

Microsoft Security Policy

Microsoft Security Policy outlines the high-level objectives related to information security, defines risk management requirements and information security roles and responsibilities. The Security Policy contains rules and requirements that are met by Azure and other Online Services staff in the delivery and operations of the Online Services environment. The Security Policy and Objectives are derived from the ISO / IEC 27001:2013 standard and is augmented to address relevant regulatory and industry requirements for the Online Services environment.

The policy is reviewed and updated, as necessary, at least annually, or more frequently, in case 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 Microsoft Security Policy and all subsequent updates are distributed to all relevant stakeholders from the Microsoft intranet site.

Roles and Responsibilities

Information security roles and responsibilities have been defined across the different Azure functions. The Cloud + AI Security team facilitates implementation of security controls and provides security guidance to the teams. The Global Ecosystem and Compliance team also coordinates with representatives from CELA (including leads of IT and Security), Human Resources (personnel security), and Microsoft Online Services (security policy requirements) on additional information security related activities impacting the services.

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 per customer requirements, as applicable. 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.

The Microsoft Online Services Delivery Platform Group works with Microsoft Human Resources and vendor companies to perform the required background check on each new or transferred personnel before they are granted access to the Microsoft Online Services production assets containing customer data.

Corporate policies are communicated to employees and relevant external parties during the onboarding process and as part of the annual security training and awareness education program. Non-disclosure Agreements (NDAs) are signed by employees and relevant external parties upon engagement with Microsoft. Disciplinary actions are defined for persons who violate the Microsoft Security Policy or commit a security breach. Employees are also required to comply with relevant laws, regulations and provisions regarding information security remain valid if the area of responsibility changes or the employment relationship is terminated. 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 employees, contractors, datacenter personnel, 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 employees at the time of joining as part of induction. In addition, all staff participate in a mandatory security, compliance, and privacy training periodically in order to design, build and operate secure cloud services.

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

Objective 1	The learner will be able to articulate the need to protect confidentiality, integrity, and availability of the production environment.
Objective 2	The learner will be able to apply basic security practices to safeguard and handle the production environment and customer information.
Objective 3	The learner will understand the criticality of security, compliance and privacy in relation to customer expectations.
Objective 4	The learner will have a basic understanding of the responsibility to meet compliance and privacy commitments.
Objective 5	The learner will know where to find additional information on security, privacy, business continuity / disaster recovery and compliance.

All Engineering staff are required to complete a computer-based training module when they join the team. Staff are required to retake this training at least once per fiscal year.

In addition, annual SBC training is mandatory for all Microsoft employees. The SBC training includes an anti-corruption section that focuses on Microsoft's anti-corruption policies and highlights policies that reinforce the need for employees to work with integrity and to comply with the anti-corruption laws of the countries in which Microsoft operates. All active employees are required to complete this course.

Information System Review

Azure 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 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 compliance requirements are monitored and reviewed regularly with CELA and other internal organizations, as applicable. Members of the Global Ecosystem and 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 Global Ecosystem and 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.

Risk Management

Azure 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.

Azure performs a cryptography risk assessment for encryption and key management to evaluate changes and updates to cryptography controls. Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within the Azure 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.

Operator Access

Production Infrastructure Access Management

Identity and Access Management (Microsoft Personnel)

The 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 uses a specific corporate AD infrastructure for centralized authentication and authorization to restrict access to the systems and services within the Azure environment. Each user account is unique and is identifiable to an individual user.

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 addition of individual user accounts to established domain security groups within the AD. Access requests to domain security groups require explicit approval from the assigned security group owner. Requests requiring explicit approval are automatically forwarded to the security group owner for approval in the system.

In addition, Azure Government access requires explicit approval with required screening to confirm US citizenship of the user that is requesting access.

Employee status data from Microsoft HR is used to facilitate the provisioning and removal of user accounts in Azure-managed AD 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 the user accounts for terminated users from the AD.

Automated mechanisms have been implemented to manage the appropriateness of access granted to information systems. Manual periodic reviews of individual accounts and security group memberships on assets are performed by authorized individuals, as appropriate, to evaluate whether access is still required. Remediation action is taken, as necessary, based on the review.

Policies and standards have been established and implemented to enforce appropriate user account password expiration, length, complexity, and history. Multi-factor authentication is enforced for production domains that do not require password-based authentication. Azure personnel are required to follow the Microsoft password policy for applicable domains as well as local user accounts for all assets. Additionally, domain user accounts, if inactive for more than 90 days, are suspended until the appropriateness of continued access for these accounts is resolved. If no action is taken by the user to reenable the suspended account, after 15 days the account is deleted.

Access to Azure Components

Access to the Azure components (e.g., Fabric, Storage, Subscriptions, and Network Devices) in the production environment is controlled through a designated set of access points and restricted to the corresponding service Production Support and Engineering teams. 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.

Access to network devices in the scope boundary requires two-factor authentication. Passwords used to access Azure network devices are restricted to authorized individuals and system processes based on job responsibilities and are changed on a periodic basis. 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 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.

Production assets that are not domain-joined or require local user accounts for authentication, require unique identifiers tied to individual user that requires appropriate approvals prior to being granted access. Non-domain-joined user accounts, that are not required due to termination of user or change in user’s role and responsibilities, are removed manually within a stipulated period of termination / role change. In addition, access through persistent interactive local accounts on servers are not considered within user access as they are configured to raise security alert upon creations and are created on isolated VMs which tend to have a short life span.

Packet Filtering

Azure has implemented filtering platform with rule sets and guards to ascertain that the untrusted VMs cannot generate spoofed traffic, cannot receive traffic not addressed to them, cannot direct traffic to protected infrastructure endpoints, and cannot send or receive inappropriate broadcast traffic.

VM based switch is designed and implemented through the filtering platform with Address Resolution Protocol (ARP) guards / rules to defend against ARP spoofing and related attacks. The guards / rules can be enabled on a per port basis to verify the sender's Media Access Control (MAC) Address and IP address to prevent spoofing of outgoing ARP packets, and only allow inbound ARP packets to reach a VM if they are targeted at that VM's IP address.

Storage nodes run only Azure-provided code and configuration, and access control is thus narrowly tailored to permit legitimate customer, applications, and administrative access only.

Virtual Local Area Network Isolation

Virtual Local Area Networks (VLANs) are used to isolate FC and other devices. VLANs partition a network such that no communication is possible between VLANs without passing through a router.

The Azure network in any datacenter is logically segregated into the Fabric core VLAN that contains trusted FCs and supporting systems and a VLAN that houses the rest of the components including the customer VMs.

Platform Secrets

Platform secrets, including certificates, keys, and Storage Account Keys (SAKs) are used for internal communication and are managed in a secure store that is restricted to authorized Azure personnel.

Access to Customer Virtual Machines by Azure Personnel

By default, user accounts are not created, and the Windows default administrator account is disabled on customer PaaS VMs. However, access to the customer VMs may be required for exceptional situations such as troubleshooting issues and handling incidents. In order to resolve these types of issues, temporary access procedures have been established to provide temporary access for Azure personnel to customer data and applications 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.

Network Device Remote Access

Azure network device access is provided through TACACS+ and local accounts, and follows standard logical access procedures as established by the Azure Networking team.

Directory and Organizational Identity Services Access Management

Customer Authentication Credentials

Each online customer is assigned a unique identity. Appropriate password hashing algorithms are in place to ensure that the authentication credential data stored is protected and is unique to a customer.

Remote Desktop

Production servers are configured to authenticate via AD. Directory and Organizational Identity Services' production servers require users to perform two-factor authentication using a smart card and domain password to gain access to the Microsoft Directory Store production servers using the Remote Desktop Connection application. Remote Desktop Connection has encryption settings enforced. These settings are controlled using the domain group policy within the production servers. The settings enforce remote desktop connections made to the production server to be encrypted.

Data Security

Data Classification and Confidentiality Policy

Data (also referred to as information and asset) is classified into twelve categories, as described in the Data section above, based on how it is used or may be used within the Service environment.

There is one other type of data which is sometimes referenced in relation to data classification and protection. Azure does not treat this as a single category. Instead, it may contain data from one or more data classes described in the Data section above.

- **Personally Identifiable Information (PII):** Any data that can identify an individual is PII. Within Azure, PII of Azure subscription / tenant administrators (direct customers) is treated differently from the PII of end-users of services hosted in Azure. This is because in order to provide the Azure service, access to Administrator PII is needed, such as in the event of outage related notifications.

The General Data Protection Regulation (GDPR) introduces new rules for organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data for EU residents no matter where they are located.

Cryptographic Controls

Cryptographic controls and approved algorithms are used for information protection within the Azure platform and implemented based on the Azure Cryptographic Policy and Microsoft Cryptographic Standards. Cryptographic keys are managed throughout their lifecycle (e.g., ownership, generation, storage, distribution, periodic rotation, revocation, deactivation and archival) in accordance with established key management procedures. Access to cryptographic keys is restricted through security groups membership and use of JIT. Azure provides customers the ability to manage their own data encryption keys.

Backup

Processes have been implemented for the backup of critical Azure components and data. Backups are managed by the Azure Data Protection Services (DPS) team and scheduled on a regular frequency established by the respective component teams. The DPS team monitors backup processes for failures and resolves them per documented procedures to meet required backup frequency and retention. Azure teams that support the services and the backup process conducts integrity checks through standard restoration activities. Further, production data is encrypted on backup media.

Backup restorations are performed periodically by appropriate individuals. Results of the test are captured and any findings are tracked to resolution.

Offsite backups are tracked and managed to maintain accuracy of the inventory information. Azure is moving from offsite tape-based storage solutions to use of storage accounts in regions or locations different from the primary data location.

Access to backup data follows the same procedures defined under the Operator Access section above.

Data Protection Services

The DPS group has implemented a secure backup system infrastructure to provide secure backup, retention, and restoration of data in the Microsoft Online Services environment. Data is encrypted prior to backup and in transit where applicable, and can be stored on tape, disk, or Storage accounts based on the service requirements.

Data Redundancy and Replication

Azure Storage provides data redundancy to minimize disruptions to the availability of customer data. The data redundancy is achieved through fragmentation of data into extents which are copied onto multiple nodes within a region. This approach minimizes the impact of isolated Storage node failures and loss of data.

Critical Azure components that support delivery of customer services have been designed to maintain high availability through redundancy and automatic failover to another instance with minimal disruption to customer services. Agents on each VM monitor the health of the VM. If the agent fails to respond, the FC reboots the VM. In case of hardware failure, the FC moves the role instance to a new hardware node and reprograms the network configuration for the service role instances to restore the service to full availability.

Customers can also leverage the geographically distributed nature of the Azure infrastructure by creating a second Storage account to provide hot-failover capability. In such a scenario, customers may create custom roles to replicate and synchronize data between Microsoft facilities. Customers may also write customized roles to extract data from Storage for offsite private backups.

Data is backed up to a region or location different from the primary data location and retained as per the retention policy.

Azure Storage maintains three replicas of customer data in blobs, tables, queues, files, and disks across three separate fault domains in the primary region. Customers can choose to enable geo-redundant storage, in which case three additional replicas of that same data will be kept also across separate fault domains in the paired region within the same geography. Examples of Azure Regions are North and South US or North and West Europe. These regions are separated by several hundred miles. Geo-replication provides additional data durability in case of a region wide disaster. For Azure Government, the geo-replication is limited to regions within the United States.

For Azure SQL that relies on Service Fabric, there are a minimum of three replicas of each database - one primary and two secondary replicas. If any component fails on the primary replica, Azure SQL detects the failure and fails over to the secondary replica. In case of a physical loss of the replica, Azure SQL creates a new replica automatically.

All critical platform metadata is backed up in an alternate region several hundred miles from the primary copy. Backup methods vary by service and include Azure Storage geo-replication, Azure SQL geo-replication, service-specific backup processes, and backup to tape. Azure manages and maintains all backup infrastructure.

Data Segregation

Directory Services assigns each tenant a unique identifier as part of the Active Directory. The mapping between the tenant and the AD location is represented within the partition table and is hidden from each customer tenant. Each tenant is segregated and partitioned within AD forest(s) based on this unique identifier to ensure appropriate customer data segregation.

Customer Data Deletion

Customer metadata is collected, retained, and removed based on documented procedures. Customer data is retained in the Online Service in a limited function account for 90 days after expiration or termination of customer’s subscription so that the customer may extract the data. After the 90 day retention period ends, the customer’s account is disabled and the customer’s data is deleted. In accordance with applicable retention policies and legal / regulatory requirements as described in the Customer Registration section of the subscription, customer data is securely disposed of upon customer instruction. Hard disk and offsite backup tape destruction guidelines have been established for appropriate disposal. Customer accounts in non-payment or in violation of terms, etc., are subject to involuntary terminations and account disablement.

Platform Communication and Customer Secrets Protection

Data integrity is a key component of the Azure Platform. Customer secrets such as Storage Account Keys are encrypted during storage and transit. The customer facing portals and APIs only allow access to the Azure platform over a secure channel based on the service.

Azure Platform Communication

Internal communication between key Azure components where customer data is transmitted and involved is secured using SSL and TLS. SSL and TLS certificates are self-signed, except for those certificates that are used for connections from outside the Azure network (including the Storage service and the FC). These certificates are issued by a Microsoft Certificate Authority. Customer data is transmitted over a secure channel to the Azure platform services.

Customer Secrets

Customer secrets, including certificates, private keys, RDP passwords and SAKs are communicated through the SMAPI via the REST protocol, or Azure Portal over a secured channel using SSL. Customer secrets are stored in an encrypted form in Azure Storage accounts. Customer secrets are only known to the customer. Further, private root keys belonging to Azure services are protected from unauthorized access.

Access Control Service Namespace

Customers interact with the Access Control Service namespace over the web and service endpoints. Access Control Service namespace is only accessible through HTTPS and uses SSL to encrypt transmission of customer secrets including cryptographic keys, passwords and certificates over external networks. The customer information transmitted to all the Access Control Service endpoints is encrypted over external networks.

Change Management

The Change Management process has been established to plan, schedule, approve, apply, distribute, and track changes, including emergency 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.

The change management process requires changes to be submitted per a pull request which is then checked into a production build once secondary review and approval is obtained. The production build then undergoes release testing, review and deployment approval prior to being released to Azure production environments.

Separation of Environments

Azure has implemented segregated environments for development, test and production, as a means to support segregation of duties and prevent unauthorized changes to production. Azure maintains logical and / or physical separation between the DEV (development), TEST (pre-production) and PROD (production) environments. Virtual services run on different clusters in separate network segments. TEST and PROD environments reside in separate network segments, which are accessed through distinct TEST and PROD Jumpboxes. Access to TEST and PROD Jumpboxes is restricted to authorized personnel from the service Operations and Production Support teams.

Deployment of software to production must meet testing and operational readiness criteria at each pre-production and production stage, and be approved prior to release. Production deployments use approved software builds and images.

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.

Segregation of Duties

Segregation of duties is established on critical functions within the Azure environment, to minimize the risk of unauthorized changes to production systems. Responsibilities for requesting, approving and implementing changes to the Azure environment are segregated among designated teams.

Software and Configuration Changes

Software and configuration changes within Azure, including major releases, minor releases, hot fixes, and emergency changes are managed through a formal change and release management procedure, and tracked using a centralized ticketing system. The categorization of these changes is based on priority and risk associated with the change. Changes are requested, approved, tracked and implemented throughout the release lifecycle, which includes product and engineering planning, release management, deployment and post-deployment support phases. Change requests are documented, assessed for their risks and evaluated / approved for acceptance by the designated Azure personnel. Software releases are discussed, planned, and approved through the daily coordinated meetings with appropriate representatives from the service and component teams.

Changes that are made to the source code are controlled through an internal source code repository. Refer to the Secure Development section for the controls enforced on the source code. Applicable operational security and internal control requirements are documented and implemented for Azure services based on Microsoft SDL methodology.

Formal security and quality assurance testing is performed prior to the software release through each pre-production environment (i.e., development and stage) based on defined acceptance criteria. The results of the quality assurance testing are reviewed and approved by the appropriate representatives prior to moving the release to production. For changes being deployed to the sovereign clouds, the change is tested in an Azure pre-production environment which is then deployed to the sovereign cloud production environment by the sovereign cloud data custodian after obtaining an additional approval from the sovereign cloud operator(s). Changes are reviewed for their adherence to established change and release management procedures prior to closure. Once deployed, 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.

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 has implemented tools to perform integrity verification checks to detect unauthorized changes to software, firmware and information.

Hardware Changes

Hardware changes are managed through formal change and release management procedures and a centralized ticketing system. Hardware changes are evaluated against the release entrance criteria that are established by the Azure Build-Out team, which forms the acceptance criteria for build-out of hardware within the Azure environment. Similar to software changes, the infrastructure changes are discussed and planned through the daily coordinated meetings with representatives from service and component teams.

The Azure Build-Out team coordinates scheduling of the release and deployment of the change into the production environment. The Azure Build-Out team performs the build-out of hardware devices and post build-out validation in coordination with the Azure Deployment Engineering team to verify its adherence to the hardware build requirements for new clusters. Azure Operations Managers perform final review and sign off of new deployments and Azure Build-Out team closes the ticket.

Network Changes

The Azure teams have implemented a formal change management process and centralized ticketing tool to document network changes and their approvals. Network changes include configuration changes, emergency changes, ACLs changes, patches, and new deployments.

ACL changes, that are identified and categorized as a standard change, are considered as pre-approved and may be implemented on peer review. Non-standard changes are reviewed for their characteristics and risks, and approved by representatives from the Cloud + AI Security and Networking teams, during the daily coordinated meeting. Reviews and approvals are also tracked in a centralized ticketing system. Changes are performed through approved change implementers that are part of a designated security group. Post-implementation reviews are performed by qualified individuals, other than the implementer, who evaluate the change success criteria.

Software Development

Secure Development

Azure's software development practices, across each of the component teams, are aligned with the Microsoft SDL methodology. The SDL introduces security and privacy control specifications during the feature / component design and throughout the development process, which are reviewed through designated security roles. The SDL review for each service is performed on an annual basis.

The Cloud + AI Security team creates the SDL baseline for Azure services to follow. The SDL baseline includes tasks to be performed which identify tools or processes that ensure teams are developing their services in a secured manner. As part of onboarding onto the SDL process, the Cloud + AI Security team works with the service teams to determine any additional SDL steps to be performed specific to the service. Additionally, teams are required to perform threat modeling exercises which are reviewed and approved by the Cloud + AI Security team. Each team has an SDL Owner who is responsible for ensuring appropriate completion of the SDL tasks. The SDL Owner reviews the SDL tasks and gives the overall sign off for completion of the SDL process.

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

Source Code Control

The Azure source code is stored within Azure's internal source code repository tools that function as the versioning system for the source code. The tools track the identity of the person who checks source code out, and what changes are made. Procedures are established to approve source code changes made to source code repository. In addition, source code builds are scanned for malware prior to production release.

Vulnerability Management

Logging and Monitoring

The Cloud + AI Security team has implemented agent-based monitoring infrastructure or custom script-based monitoring within the Azure environment to provide automated logging and alerting capabilities. The logging solutions are enabled on all production systems. 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 abnormal log information to a centralized log repository either at regular intervals or in real-time. Availability of logging and monitoring software is monitored by internal tools on a continuous basis, and responsible personnel are 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. Additionally, Azure has implemented an Immutable Log engine within the Geneva Monitoring platform to help ensure the integrity of security logs stored at rest with minimal risk of the data being deleted or modified. This is achieved through a configuration policy that defines which security events are considered immutable (cannot be deleted or modified) and the number of days logs are retained (in immutable state) prior to deletion. Azure has also implemented automated processes to detect instances where immutability has not been configured and sends alerts notifying the service teams to take corrective action. Immutability configurations are owned by the Geneva Monitoring team and can only be changed through the standard change management process ensuring segregation of duties.

Component teams (e.g., Fabric and Storage) determine the specific events that need to be captured in consideration with a baseline. Administrator, operator, and system activities performed, such as logon / logoff within the Azure environment, are logged and monitored. As such, Azure components are configured to use Coordinated Universal Time (UTC) time and the clocks are synchronized with the domain controller server.

For network devices, the Azure Networking team monitors, logs, and reports on critical / suspicious activities and deviations from established baseline security configuration for the network devices. Predefined events are reported, tracked, and followed up on and security data is available for forensic investigations. The logs are retained centrally for forensic related analysis and access to the logs follows the same procedures defined under Operator Access section above.

The Cloud + AI Security team has implemented an alerting system to provide real-time alerting through automatic generation of emails and alarms based on the log information captured by the monitoring infrastructure. Component teams are responsible for configuring the events to be alerted. The event and warning logs are routinely examined for anomalous behavior and when necessary, appropriate actions are taken in accordance with the incident handling procedures described in the Incident Management section. The Cyber Defense Operations Center (CDOC), Azure Live Site, and component teams manage response to malicious events, including escalation to and engaging specialized support groups. In addition, the CDOC interacts and communicates with relevant external parties to stay up-to-date and share current threat scenarios and countermeasures.

Azure provides logging mechanisms that can be configured by customers to log activities and performance metrics related to their resources.

System Monitoring Tools

1. Geneva Monitoring within the Azure platform provides automated centralized logging and alerting capabilities for monitoring system use and detection of potential unauthorized activity. The Geneva Monitoring capabilities include Data Collection, Data Aggregation, Data Analysis and Information Access.

2. Alert and Incident Management System (IcM) provides alerting on a real-time basis by automatically generating emails and incident tickets based on the log information captured in Geneva Monitoring.
3. Azure Security Monitoring (ASM) provides logging and alerting capabilities upon detection of breaches or attempts to breach Azure platform trust boundaries. Critical security event logs generated are configured to alert through IcM. ASM monitors key security parameters to identify potentially malicious activity on Azure nodes.
4. Microsoft Endpoint Protection (MEP) guards against malware and helps improve security of the Azure PaaS Guest customers, Azure infrastructure tenants and Azure internal applications. MEP can be configured to enable antimalware protection for the Azure infrastructure tenants and Azure PaaS Guest VMs. 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 takes action to remove the detected threat.
5. System Center Endpoint Protection (SCEP) guards against malware and helps improve security for Azure IaaS and physical servers. SCEP solution is designed to run in the background and check for updates at least daily without requiring human intervention. If malware is detected, the endpoint protection agent automatically takes action to remove the detected threat.
6. ClamAV is implemented to monitor for malicious software in the Linux based server environment. ClamAV performs at least daily checks for updates. If malware is detected, the endpoint protection agent automatically takes action to remove the detected threat.
7. Windows Defender guards against malware and helps improve security of the Azure PaaS, IaaS, and physical servers running Windows Server 2016 and newer. Windows Defender can be configured to enable antimalware protection for the Azure infrastructure tenants and Azure PaaS Guest VMs. 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 Live Site team uses third-party external monitoring services to monitor service health and performance (including the logging and monitoring tools).

Network Monitoring

The Networking team maintains a logging infrastructure and monitoring processes for network devices. In addition, the Azure Live Site team uses WaNetMon and third-party external monitoring services to monitor network connectivity. In addition, OneDDoS service is implemented on the Azure network to detect and respond to network-based attacks.

Vulnerability Scanning

Cloud + AI Security team carries out frequent internal and external scans to identify vulnerabilities and assess the effectiveness of the patch management process. Services are scanned for known vulnerabilities; new services are added to the next timed quarterly scan, based on their date of inclusion, and follow at least a quarterly scanning schedule thereafter. These scans are used to ensure compliance with baseline configuration templates, validate that relevant patches are installed and identify vulnerabilities. The scanning reports are reviewed by appropriate personnel and remediation efforts are conducted in a timely manner.

Patching

The service and component teams are notified by the Microsoft Security Response Center (MSRC) upon identification of technical vulnerabilities applicable to the Azure Windows-based systems. Azure works with MSRC to evaluate patch releases and determine applicability and impact to Azure and other Microsoft Online Services environments and customers. For Linux based systems, the Ubuntu Security Notices for Linux patches are relied upon as the primary source. The applicable security patches are applied immediately or during a scheduled release to the Azure environment based on the severity of the vulnerability.

Processes are in place to evaluate patches and their applicability to the Azure environment. Once patches have been reviewed and their criticality level determined, service teams determine the release cadence for implementing patches without service disruption.

Applicable patches are automatically applied to Guest PaaS VMs unless the customer has configured the VM for manual upgrades. In this case, the customer is responsible for applying patches.

Teams follow a change process to modify the underlying OS within the platform. All changes are reviewed and tested, at a minimum, for their quality, performance, impact on other systems, recovery objectives and security features before they are moved into production using a defined release process. Test windows have been established for reviewing and testing of new features, and changes to existing features and patches.

Patches are released through the periodic OS release cycle in accordance with change and release management procedures. Emergency out-of-band security patches (e.g., Software Security Incident Response Process patches) are expedited for more immediate release.

Securing Edge Sites

All drives and operating systems used for production servers that reside in edge locations are encrypted. The drives have 'Always On' encryption and stay encrypted even during OS patching and updates. In addition, all unused IO ports on production servers that reside in edge locations are disabled by OS-level configurations that are defined in the baseline security configuration. Continuous configuration validation checks are enabled to detect drift in the OS-level configurations.

In addition, intrusion detection switches are enabled to detect physical access of the device. An alert is sent to an operator and the affected servers are shut down and its secrets are revoked. The alerting and tracking follows the incident response process as defined below.

Penetration Testing

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

Incident Management

Azure 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. Azure reviews the vulnerability and incident management standard operating procedures annually. Azure reviews the implementation of these procedures as part of their internal monitoring and changes are made as often as needed to support continuous improvement of these processes and procedures.

Security Incident - Internal Monitoring and Communication

Azure has established incident response procedures and centralized tracking tools which consist of different channels for reporting production system incidents and weaknesses. Automated mechanisms include system monitoring processes for alerting the Azure Live Site, CDOC, and service On-Call teams per defined and configured event, threshold or metric triggers. Incidents may also be reported via email by different Azure or Microsoft groups such as the service and component teams, Azure Support team or datacenter teams. Users are made aware of their responsibilities of reporting incidents that shall be looked into without any negative consequences. The Azure Live Site, CDOC, and service On-Call teams provide 24x7 event / incident monitoring and response services. The teams assess the health of various components of Azure and datacenters, along with access to detailed information when issues are discovered. Processes are in place to enable temporary access to customer VMs. Access is only granted during, and for the duration of, a specific incident.

Additionally, CDOC conducts yearly tests of the Incident Management SOPs and response capabilities. Reports related to information security events are provided to Azure management on a quarterly basis. Problem statements for systemic issues are submitted to Information Security Management Forum for executive leadership review.

Incident Handling

Azure teams use 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 Live Site and CDOC teams, with assistance from additional Azure teams (e.g., Cloud + AI Security team, component teams for investigation, when necessary), document, track, and coordinate 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 or incidents with high severity ratings (i.e., levels 0 and 1). The post-mortems are reviewed by the Azure Operations Management team during weekly and monthly review meetings with Azure senior management. Incident and security post-mortem trends are reviewed and evaluated on a periodic basis and, where necessary, the Azure platform or security program may be updated to incorporate improvements identified as a result of incidents.

Network Problem Management

The Networking team comprises Problem Management, Network Escalations, and Network Security teams to identify and address security alerts and incidents. The Networking team is responsible for identifying and analyzing potential problems and issues in the Microsoft Online Services networking environment.

Physical and Environmental Security

Datacenter Services

The Datacenter Management team has overall responsibility for the oversight of datacenter operations, including physical security, site services (server deployments and break-fix work), infrastructure build-out, critical environment operations and maintenance, and facilities management. Site Security Officers are responsible for monitoring the physical security of the facility 24x7x365.

Third-party vendors may perform various services in a Microsoft datacenter. For example:

- Mission critical vendors may be responsible for maintaining the datacenter's critical environment equipment.
- Security vendors may manage the site security guard force.
- General facilities management vendors may be responsible for minor building-related services, such as telephones, network, cleaning, trash removal, painting, doors, and locks.
- Site Services may support the Microsoft Online Services operations.

Datacenter Physical Security Management reviews and approves the incident response procedure on a yearly basis. The security incident response procedure details the appropriate steps to be taken in the event of a security incident and the methods to report security weaknesses.

Physical Security

Main access to the datacenter facilities are typically restricted to a single point of entry that is manned by security personnel. The main interior or reception areas have electronic card access control devices on the perimeter door(s), which restrict access to the interior facilities. Rooms within the Microsoft datacenters that contain critical systems (servers, generators, electrical panels, network equipment, etc.) are restricted through various security mechanisms, such as electronic card access control, keyed lock on each individual door, man traps, and / or biometric devices.

Access Controls

The Datacenter Management team has implemented operational procedures to restrict physical access to only authorized employees, contractors, and visitors. Temporary or permanent access requests are tracked using a ticketing system. Badges are either issued or activated for personnel requiring access after verification of identification. The Datacenter Management team is responsible for reviewing datacenter access on a regular basis and for conducting a quarterly audit to verify individual access is still required.

Datacenter Security Personnel

Security personnel in the datacenter conduct the following activities for various datacenter facilities:

1. Man the security desks located at the main entrance of the datacenter
2. Conduct periodic inspections of the datacenter through walkthroughs
3. Respond to fire alarms and safety issues
4. Dispatch security personnel to assist service requests and emergencies
5. Provide Datacenter Management team with periodic updates about security events and entry logs
6. Operate and monitor datacenter surveillance systems

Security Surveillance

Datacenter surveillance systems monitor critical datacenter areas like datacenter main entry / exit, datacenter co-locations entry / exit, cages, locked cabinets, aisle ways, shipping and receiving areas, critical environments, perimeter doors, and parking areas. Surveillance recordings are retained for 90 days or as the local law dictates.

Emergency Power and Facility and Environmental Protection

Microsoft datacenter facilities have power backup and environmental protection systems. Datacenter Management team or the contracted vendor performs regular maintenance and testing of these systems.

Logical Access

Customer Data and Systems Access Management (Customers)

Customer Registration

Azure customers register for Azure services by setting up a subscription through the MOCP using a Microsoft Account or Organizational Account. Additionally, depending on the service, customers have the ability to register for the service via the service specific portal. MOCP, including billing and registration, and Microsoft Account / Organizational Account, including password management, are not in scope of this SOC report.

After registration, customers can request the creation of Storage accounts, hosted services, tenants, roles, and role instances within their subscription using the Azure Portal or programmatically through the SMAPI, which is the HTTPS interface exposed to external customers. The SMAPI allows customers to deploy and manage their services and their account. Among other things, this involves the ability to modify hosted services and Storage accounts, pick the geo-location for these accounts and place them in affinity groups, update configurations, 'swap' deployments and in essence, do all the non-creation related deployment / management operations that customers can do through the Azure Portal.

Additionally, customers can utilize the Microsoft Entra ID Graph API for programmatic access to Microsoft Entra ID through REST API endpoints. Applications can use the Graph API to perform create, read, update and delete (CRUD) operations on directory data and objects, e.g., common operations for a user object like create new users in directory, get user details, update user properties, and ascertain role-based access for user's group membership. Customers can also use the Microsoft Entra ID Module for Windows PowerShell cmdlets (provisioning API) to automate a number of deployment and management tasks. Azure has published a standard set of APIs with an ecosystem of tools and libraries on the Microsoft public website. All APIs or SDKs that services offer must be documented for inoperability and portability.

Virtual Machine Customization

Upon creation of a VM, the VM image includes customizations to performance, security and productivity. However, the image may be customized further by the customer to suit their needs. Hardening of the image is the responsibility of the customer. Access to the images may be restricted by the customer and updates to available images are communicated through customer-facing websites.

Identity and Access Management

Access to the Azure subscription through the Azure Portal is controlled by the Microsoft Account / Organizational Account. The ability to authenticate with the Microsoft Account / Organizational Account associated with the Azure subscription grants full control to all of the hosted services and Storage accounts within that subscription. (Note: Microsoft Account / Organizational Account and its associated authentication mechanisms are not in scope of this SOC report).

User sessions in the Azure portal can be configured by customers to automatically sign the user out of the Azure Portal session after a stipulated period of inactivity, protecting resources from unauthorized activity. The session will automatically terminate when the device's active focus is not on the Azure Portal for the stipulated period defined in the "Signing out + notifications" settings.

Location awareness technologies are implemented as part of the Azure Portal where location of the machine used for authentication is factored into the validation of the user identity. Where the user identity cannot be validated, Azure Portal would require the user to provide additional information to confirm their identity that could include MFA and / or secondary contact information for verification.

Applications can also access Azure services by using APIs (also known as SMAPI). SMAPI authentication is based on a user-generated public / private key pair and self-signed certificate registered through the Azure Portal. It is the customer's responsibility to safeguard the certificate.

The certificate is then used to authenticate subsequent access to SMAPI. SMAPI queues request to the Fabric, which then provisions, initializes, and manages the required application. Customers can monitor and manage their applications via the Azure Portal or programmatically through SMAPI using the same authentication mechanism.

In addition, customers can enable defined ports and protocols, e.g., RDP or SSH for Linux based services, on their instances and create local user accounts through the Azure Portal or SMAPI for debugging / troubleshooting issues with their applications. Customers are responsible for managing the local user accounts created.

Logic Apps allows users to run jobs such as calling HTTP/S endpoints or posting messages to Azure Storage queues on any schedule. Jobs can be integrated with user applications and can be configured to run immediately, or on a recurring schedule or anytime in the future. Jobs can be configured to call services both inside and outside of Azure. Jobs are processed as per the job settings defined by the customer. In case an error occurs during the processing, the job is retried based on the retry interval as mentioned by the customer. Errors are monitored and appropriate action is taken based on the settings defined by the customer. Jobs configured by customer administrators are executed within thirty (30) minutes of the scheduled job run and are repeated based on the defined recurrence settings.

Azure Automation allows users to create, monitor, manage, and deploy resources in the Azure environment using runbooks. These runbooks can be configured and schedules can be created to automate the manual, long-running, error-prone, and frequently repeated tasks that are commonly performed in a cloud environment.

Services initialize the resource groups within the Azure Portal based on the customer configured templates. A customer tenant can create an Azure Resource Manager using an ARM template. The template deploys and provisions all resources for any application in a single, coordinated operation. In the template, a customer tenant can define the resources that are needed for the application and specify deployment parameters to input values for different environments. The template consists of JSON and expressions which the customer tenant can use to construct values for their deployment. Later, these resources under ARM can be accessed, monitor utilization, and reconfigure based on capacity utilization using the deployment parameters that were entered during ARM creation. Further, customer data is accessible within agreed upon services in data formats compatible with providing those services.

Access to Customer Virtual Machines

External traffic to customer VMs is protected via ACLs but can be configured by the customer to allow external traffic only to customer designated ports and protocols. There is no port that is open by default unless explicitly configured by the customer in the service definition file. Once configured, the Azure Fabric Controller automatically updates the network traffic rule sets to allow external traffic only to the customer designated ports.

Customers can connect to their VMs via the ports and protocols defined by them, create credentials (i.e., username and password) and choose a certificate to encrypt the credentials during initial set-up that expires within 14 days through a secured mechanism. Authentication after set-up is performed using the self-created credentials. The connection is secured via Transport Layer Security (TLS) using a self-signed certificate generated by the VM instance. Customers can also upload custom certificates via the Azure Portal and configure their instances to use them securely.

Access to Customer Storage Account Data

Access to Azure Storage (i.e., blobs, tables, queues, files and disks) is governed by the SAK that is associated with each Storage account. Access to the SAK provides full control over the data in the Storage account.

Access to Azure Storage data can also be controlled through a Shared Access Signature (SAS). The SAS is created through a query template (URL), signed with the SAK. That signed URL can be given to another process, which can then fill in the details of the query and make the request of the Storage service. Authentication is still based on a signature created using the SAK, but it is sent to the Storage server by a third party. Access using the SAS can be limited in terms of validity time, permission set and what portions of the Storage account are accessible.

Data security beyond the access controls described above, such as fine-grain access controls or encryption, is the responsibility of the customer with exception to Managed Disk where encryption is enabled by default.

Identity and Access Management - Self Service Password Reset

Self-Service Password Reset (SSPR) for users is a feature which allows end-users in customer organization to reset their passwords automatically without calling an administrator or helpdesk for support. SSPR has three main components:

1. **Password Reset Policy Configuration Portal** - Administrators can control different facets of password reset policy in the Azure Portal.
2. **User Registration Portal** - Users can self-register for password reset through a web portal.
3. **User Password Reset Portal** - Users can reset their own passwords using a number of different challenges in accordance with the administrator-controlled password-reset policy.

Customer Administrative Passwords

The One Time Password (OTP) generation module is implemented as a worker role within the Azure AD platform and OTP used for self-service password reset are randomly generated. These OTPs expire after their usage or a pre-defined time limit. OTP generated for email and SMS are validated. Additionally, the OTP values are to be provided within the same session where the OTP was requested.

For the password reset process, the only information displayed within the HTTPS response packets is the masked phone number and cookies required to reset the password. The new passwords supplied by customer administrators within the SSPR portal adhere to the Azure AD password policy requirements. The SSPR portal is only accessible through HTTPS port and the new passwords supplied by the customers are encrypted during transmission over external networks.

This also applies to the initial temporary password generated for the user. These temporary passwords have a pre-defined time limit before it expires and forces users to change it on first usage.

Quotas and Thresholds

Where applicable, quotas are enforced on Azure services as configured by the service administrators. Quota name, the threshold value for the quota, and the behavior on exceeding the quota, have been specified to protect customer entities from availability related issues.

Business Continuity and Resiliency

Microsoft has established an organization-wide Enterprise Business Continuity Management (EBCM) framework that serves as a guideline for developing Azure 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 Business Continuity Management (BCM) Program Manager manages the program for Azure, and the datacenter Service Resiliency (SR) program is coordinated through the datacenter SR Program Management Office to ensure that the program adheres to a coherent long-term vision and mission, and is consistent with enterprise program standards, methods, policies, and metrics.

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

The BCP and / or DRP includes scope and applicable dependencies for the services, restoration procedures, and communications with appropriate teams (i.e. Incident Management). The BCP and DRP are reviewed at least annually by a designated user and made available to all applicable users. The Business Continuity team conducts testing of the business continuity and disaster recovery plans established for Azure services, per the defined testing schedule for various loss scenarios. Each loss scenario is tested at least annually. Issues identified during testing are resolved and plans are updated accordingly.

The BCM charter provides strategic direction and leadership to various aspects of the datacenter organization. The BCM program is coordinated through the Program Management Office to ensure that the program adheres to a coherent long-term vision and mission, and is consistent with enterprise program standards, methods, policies, and metrics.

Azure Resiliency Program

Azure 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.

In scope for this plan are Azure’s critical business processes (defined as needed within 24 hours or less). These processes were determined during a BIA, in which Azure 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 the process. Following the BIA, a Non-Technical Dependency Analysis was performed to determine the specific people, applications, vital records, and user requirements necessary to perform the process. The BCP’s scope covers only the critical business processes determined during the BIA.

On a periodic basis, Azure performs testing of the BCP, or implementation of the plan due to a live event, to assess the effectiveness and usability of the BCP and to identify areas where risks can be eliminated or mitigated. Where applicable, third parties are involved in the test if there are dependencies associated with them. The results of testing are documented, validated and approved by appropriate personnel. This information is used to create and prioritize work items.

Datacenter Service Resiliency Program

As part of the datacenter SR program, the Datacenter Management team develops the methods, policies and metrics that address the information security requirements needed for the organization’s business continuity. The team develops BCPs and DRPs for the continued operations of critical processes and required resources in the event of a disruption.

Additionally, the Datacenter Management team conducts and documents a resiliency assessment specific to the datacenter’s operations on an annual basis or prior to proposed significant changes.

Capacity Management

The Networking team continually monitors the network to ensure availability and addresses capacity issues in a timely manner. The process for weekly capacity review is initiated by the Network Capacity Management team. The review includes an analysis of the capacity based on various parameters and the Network Hotlist report. 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.

Third Party Management

Third parties undergo a review process through Global Procurement and an approved vendor list has been 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 MMVA, a signed NDA is also required. Vendors requiring access to source code need to be approved by the General Manager and CELA, and sign a Source Code Licensing Agreement.

Microsoft's exit strategy for critical suppliers is to have multiple suppliers readily available in case an exit is needed. Each supplier is assessed against the same indicators of success and resource requirements.

Periodic reviews are performed on third parties against their applicable SLAs and security requirements. Any findings from these reviews are tracked to resolution and / or require further reviews with the third party.

Microsoft partners with third-party companies to help meet customers' needs. These third-party companies are referred to as suppliers.

Asset Management

Azure assets are classified in accordance with Microsoft Online Services Classification guidelines. The classification process is owned by the Azure Global team. There are five categories for classification: Non-business, Public, General, Confidential, and Highly Confidential. Steps are taken to protect assets commensurate with the respective asset's classification and its data sovereignty. Review of asset inventory, ownership, and classification is performed at least semi-annually.

The Azure Scope Boundary inventory of servers is monitored and maintained by the Azure Inventory team. Azure inventory is maintained automatically ensuring complete, accurate, valid, and consistent inventory as it is automatically updated by all upstream data sources.

Azure has created and implemented processes to control the delivery and removal of information assets through a centralized ticketing system. If equipment is shipped from multiple locations, a separate ticket must be created for each location.

In addition, network architecture is maintained as part of the inventory process. Metadata of the assets is collected and maintained within the inventory that provides an overview and flow of the network.

Communications

Policies Communication

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

Service Level Agreements

Azure details commitments made regarding delivery or performance of services. These details are published in the SLAs available on the following website: https://www.microsoft.com/licensing/terms/.

Customer Communication

Prior to provisioning Azure services, customers are required to review and agree with the acceptable use of data and the Azure service, as well as security and privacy requirements, which are defined in the Microsoft Product Terms, Microsoft Online Subscription Agreement, Azure Platform Privacy Statement and Technical Overview of the Security Features in the Azure Platform.

Subsequent communication with customers is primarily achieved through the following options:

- Service Dashboard - Azure maintains and notifies customers of potential changes, events and incidents that may impact security, availability, processing integrity, or confidentiality of the services through an online Service Dashboard. The online Service Dashboard is updated in real time and RSS feeds are also available for subscription. Service Dashboard is used to disclose nature, timing, extent, and disposition of the incidents impacting various services.

- Legal - Any changes / updates to the Service Agreement, Terms, End User License Agreement (EULA), Acceptable Use Policy, Privacy Statement or SLAs are posted on the Azure website. The information presented in the Microsoft Trust Center is current as of the 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 can communicate with Azure 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, as well as the shared responsibility model that outlines responsibilities between Azure and its customers are communicated through the Microsoft Trust Center (https://www.microsoft.com/en-us/trustcenter/). Additionally, description of the services, their key components, and recommendations on secure use of those services are available to customers through the Azure Service Directory (https://azure.microsoft.com/en-us/services/). In addition, supported virtualization standards for the Azure environment are available on the Microsoft public website.

MSRC identifies, monitors, responds to, and resolves security incidents and vulnerabilities in Microsoft software. The MSRC is on constant alert for security threats, monitoring security newsgroups, and responding to reported vulnerabilities - 365 days a year. Microsoft operating system updates for virtual machines are made available through Microsoft Security Response Center (MSRC) site and Windows Update. Customers and other third parties can report suspected vulnerabilities by emailing secure@microsoft.com.

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.

Baseline Configuration

Baseline Security Configuration for Services

Technical standards and baselines have been established and communicated for OS deployments. Automated mechanisms and periodic scanning have been deployed to detect and troubleshoot exceptions and / or deviations from the baseline in the production environment. Where applicable, mechanisms are in place for services to re-image production servers with the latest baseline configuration at least on a monthly frequency. Further, OS and component teams review and update configuration settings and baseline configurations at least annually.

Network Configuration

The Networking team has implemented procedural and technical standards for the deployment of network devices. These standards include baseline configurations for network devices, network architecture, and approved protocols and ports. The Networking team regularly monitors network devices for compliance with technical standards and potential malicious activities.

Processing Integrity

Azure monitors the transactions invoked by the customer and relays them appropriately to the suitable RP end-point. RDFE, ARM and Microsoft Azure Portal utilize Azure configuration files for determining the types of events that are to be recorded when processing a transaction. Additionally, monitoring rules have been defined to process the events that have been recorded and generate alerts per the severity of an event and forward the same to the required stakeholders in the process, so they can take appropriate action. Azure management reviews portal performance monthly through 1) live site reviews performed at the service level where service teams will review all outages and incidents that occurred subsequent to the prior live site review and 2) high level live site reviews where management reviews trends and contributing factors that cause outages to evaluate the performance of Azure services against compliance with customer SLA requirements.

Requests made through Service Management API or the Azure Portal are segregated based on the subscription IDs and service requests are provisioned based on the parameters defined as per the customer's request. The request header contains the unique subscription ID of the user creating the request, the service requested and the request type allowing Azure to appropriately provision customer services. Azure performs input validation to restrict any non-permissible requests to the API which includes checking for validity of subscription IDs and the user, Denial of Service (DoS) attack mitigation, protection against XML bombs, namespace validation and header information.

System Incidents

Microsoft has publicly acknowledged cyberattacks by a state-sponsored entity known as Midnight Blizzard. Based upon information known, as of October 15, 2024, the incident associated with Midnight Blizzard did not impact the overall achievement of our service commitments and system requirements based on the trust service criteria during the period of April 1, 2024 to March 31, 2025. Microsoft concluded its investigation into the incident on October 15, 2024.

Changes to the Azure system

The changes to the Azure system from April 1, 2024 to March 31, 2025 that would affect report users' understanding of how the system is used are as follows:

- Changes were made to the offerings/services, datacenter locations, and edge sites to reflect the current scope. Refer to the updated list of offerings/services, datacenter locations, and edge sites in the "Azure and Azure Government Report Scope and Boundary" and "Regions covered by this Report" subsections in section 3 of this SOC 2 report.

Relationship between Trust Services Criteria and Description Sections

Refer to Part A in section 4 of this report for the Trust Services Criteria and the related control activities that cover those criteria.

Relationship between C5 Objectives and Description Sections

Refer to Part B in section 4 of this report for the C5 objectives and the related control activities that cover those objectives.

Section 4: 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 4: 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 April 1, 2024 through March 31, 2025. Our tests of controls were performed on controls as they existed during the period of April 1, 2024, through March 31, 2025 and were applied to those controls specified by Microsoft Corporation.

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 discrepancies 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.

Testing of tools supporting control activities

For the tools used in the performance of control activities in section 4, we performed procedures to address the risks associated with their use. While these procedures were not specifically included in the test procedures listed in section 4, they were completed as part of the testing to support our conclusions.

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 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 four parts:

Part A: Contains the Trust Services Criteria, the related 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 control activities, and the results of the testing performed.

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

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

CONTROL ENVIRONMENT

Trust Criteria	Azure Activity	Test Result
CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	**ELC - 1.** Microsoft's values are accessible to employees via the Values SharePoint site and are updated as necessary by management. **ELC - 2.** Microsoft Compliance & 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 & 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. **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. **SOC2 - 11.** Microsoft has defined disciplinary actions for employees and contingent staff that commit a security breach or violate Microsoft Security Policy. **SOC2 - 12.** 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. **SOC2 - 13.** Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees are provided Microsoft's Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage. Employees are required to acknowledge agreements to return Microsoft assets upon termination.	No exceptions noted.
CC1.2 COSO Principle 2: The board of directors demonstrates independence from	**ELC - 4.** The Audit Committee (AC) reviews its Charter and Responsibilities on an annual basis, as listed in its calendar. The AC Responsibilities include meeting	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
management and exercises oversight of the development and performance of internal control.	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. **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.	
CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	**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. **IS - 1.** A security policy that defines the information security rules and requirements for the Service environment has been established and communicated. **IS - 3.** Management has established defined roles and responsibilities to oversee implementation of the Security Policy across Azure. **SOC2 - 19.** A compliance program is managed with representation from various cross-functional teams and external parties to identify and manage compliance with relevant statutory, regulatory and contractual requirements.	No exceptions noted.
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	**ELC - 1.** Microsoft's values are accessible to employees via the Values SharePoint site and are updated as necessary by management. **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. **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.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	IS - 4. An information security education and awareness program that includes policy training and periodic security updates for Azure personnel has been established. **SOC2 - 12.** 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. **SOC2 - 13.** Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees are provided Microsoft's Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage. Employees are required to acknowledge agreements to return Microsoft assets upon termination.	
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	**ELC - 2.** Microsoft Compliance & 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 & 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. **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. **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. **IS - 2.** The Security Policy is reviewed and approved annually by appropriate management.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	IS - 3. Management has established defined roles and responsibilities to oversee implementation of the Security Policy across Azure. **SOC2 - 11.** Microsoft has defined disciplinary actions for employees and contingent staff that commit a security breach or violate Microsoft Security Policy. **SOC2 - 13.** Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees are provided Microsoft's Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage. Employees are required to acknowledge agreements to return Microsoft assets upon termination. **SOC2 - 20.** Azure performs periodic Information Security Management System (ISMS) reviews and reviews results 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. Audit activities are planned and agreed upon in advance by stakeholders and any access required to perform the audits requires approval.	

COMMUNICATION AND INFORMATION

Trust Criteria	Azure Activity	Test Result
CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	**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. **ELC - 9.** The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management. **IS - 1.** A security policy that defines the information security rules and requirements for the Service environment has been established and communicated. **SOC2 - 18.** Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements for each information system and the organization, should be explicitly defined, documented, and kept up to date. **SOC2 - 19.** A compliance program is managed with representation from various cross-functional teams and external parties to identify and manage compliance with relevant statutory, regulatory and contractual requirements. **SOC2 - 20.** Azure performs periodic Information Security Management System (ISMS) reviews and reviews results 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. Audit activities are planned and agreed upon in advance by stakeholders and any access required to perform the audits requires approval. **SOC2 - 26.** Microsoft Azure 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.	
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.	**ELC - 2.** Microsoft Compliance & 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 & 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.	No exceptions noted.

Trust Criteria	Azure 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. **IS - 1.** A security policy that defines the information security rules and requirements for the Service environment has been established and communicated. **IS - 3.** Management has established defined roles and responsibilities to oversee implementation of the Security Policy across Azure. **IS - 4.** An information security education and awareness program that includes policy training and periodic security updates for Azure personnel has been established. **SOC2 - 3.** Datacenter team controls the delivery and removal of information system components through tickets on the Global Datacenter Operations (GDCO) ticketing system. Delivery and removal of information system components is authorized by system owners. System components / assets are tracked in the GDCO ticketing database. **SOC2 - 6.** Azure maintains a Customer Support website that describes the process for customers and other external users to inform about potential security issues and submit complaints. Reported issues are reviewed and addressed per documented incident management procedures. **SOC2 - 7.** Azure 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. **SOC2 - 9.** Azure maintains and notifies customers of potential changes and events that may impact security or availability of the services through an online Service Dashboard. Changes to the security commitments and security obligations of Azure customers are updated on the Azure website in a timely manner. **SOC2 - 10.** Prior to engaging in Azure services, customers are required to review and agree with the acceptable use of data and the Azure service, as well as security and privacy requirements, which are defined in the Product Terms,	

Trust Criteria	Azure Activity	Test Result
	Microsoft Online Subscription Agreement, Azure service Privacy Statement and Technical Overview of the Security Features in Azure service. **SOC2 - 13.** Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees are provided Microsoft's Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage. Employees are required to acknowledge agreements to return Microsoft assets upon termination. **SOC2 - 14.** Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information, should be identified and regularly reviewed. **SOC2 - 19.** A compliance program is managed with representation from various cross-functional teams and external parties to identify and manage compliance with relevant statutory, regulatory and contractual requirements. **IM - 1.** An incident management framework with defined processes, roles, and responsibilities for the detection, escalation and response of incidents, has been established and communicated. **IM - 3.** The Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures.	
CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	**ELC - 2.** Microsoft Compliance & 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 & 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. **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.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	IS - 1. A security policy that defines the information security rules and requirements for the Service environment has been established and communicated. **IS - 3.** Management has established defined roles and responsibilities to oversee implementation of the Security Policy across Azure. **IS - 4.** An information security education and awareness program that includes policy training and periodic security updates for Azure personnel has been established. **SOC2 - 3.** Datacenter team controls the delivery and removal of information system components through tickets on the Global Datacenter Operations (GDCO) ticketing system. Delivery and removal of information system components is authorized by system owners. System components / assets are tracked in the GDCO ticketing database. **SOC2 - 6.** Azure maintains a Customer Support website that describes the process for customers and other external users to inform about potential security issues and submit complaints. Reported issues are reviewed and addressed by documented incident management procedures. **SOC2 - 7.** Azure 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. **SOC2 - 8.** Azure maintains and distributes an accurate system description to authorized users. **SOC2 - 9.** Azure maintains and notifies customers of potential changes and events that may impact security or availability of the services through an online Service Dashboard. Changes to the security commitments and security obligations of Azure customers are updated on the Azure website in a timely manner. **SOC2 - 10.** Prior to engaging in Azure services, customers are required to review and agree with the acceptable use of data and the Azure service, as well as security and privacy requirements, which are defined in the Product Terms,	

Trust Criteria	Azure Activity	Test Result
	Microsoft Online Subscription Agreement, Azure service Privacy Statement and Technical Overview of the Security Features in Azure service. **SOC2 - 13.** Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees are provided Microsoft's Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage. Employees are required to acknowledge agreements to return Microsoft assets upon termination. **SOC2 - 14.** Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information, should be identified and regularly reviewed. **SOC2 - 19.** A compliance program is managed with representation from various cross-functional teams and external parties to identify and manage compliance with relevant statutory, regulatory and contractual requirements. **SOC2 - 20.** Azure performs periodic Information Security Management System (ISMS) reviews and reviews results 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. Audit activities are planned and agreed upon in advance by stakeholders and any access required to perform the audits requires approval. **IM - 1.** An incident management framework with defined processes, roles, and responsibilities for the detection, escalation and response of incidents, has been established and communicated. **IM - 3.** The Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures.	

RISK ASSESSMENT

Trust Criteria	Azure 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.	**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. **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. **SOC2 - 7.** Azure 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. **SOC2 - 9.** Azure maintains and notifies customers of potential changes and events that may impact security or availability of the services through an online Service Dashboard. Changes to the security commitments and security obligations of Azure customers are updated on the Azure website in a timely manner. **SOC2 - 18.** Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements for each information system and the organization, should be explicitly defined, documented, and kept up to date. **SOC2 - 19.** A compliance program is managed with representation from various cross-functional teams and external parties to identify and manage compliance with relevant statutory, regulatory and contractual requirements. **SOC2 - 20.** Azure performs periodic Information Security Management System (ISMS) reviews and reviews results with management. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions. Audit activities are planned and agreed upon in advance by stakeholders and any access required to perform the audits requires approval. **SOC2 - 25.** Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within the Azure environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Corporate, External, and Legal Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements. **SOC2 - 26.** Microsoft Azure 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. **DS - 18.** Microsoft performs a risk assessment for encryption and key management to evaluate changes and updates to cryptography controls.	
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.	**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. **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. **BC - 1.** Business Continuity Plans (BCP) for critical Azure services, which provide roles and responsibilities and detailed procedures for recovery and reconstitution of systems to a known state per defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), have been documented and published. Plans are reviewed on an annual basis, at a minimum.	**Exception noted:** **VM - 6:** Internal Audit of Microsoft identified multiple vulnerabilities associated with five in-scope services that were not remediated in a timely manner within the expected SLA. No additional exceptions were noted in our independent testing.

Trust Criteria	Azure Activity	Test Result
	BC - 5. Risk assessments are conducted to identify and assess business continuity risks related to Azure services. **BC - 7.** A Datacenter Business Continuity Management (BCM) program to respond to Microsoft's Enterprise Business Continuance Initiative has been implemented and includes documented procedures for mapping processes to pre-defined enterprise functions, establishing recovery strategies as well as developing and conducting test scenarios that enable the BCM program to mitigate risks and vulnerabilities and respond to major disruptive events. **BC - 8.** A Datacenter Business Continuity Management Program defines business continuity planning and testing requirements for functions within the datacenters. Datacenters exercise, test and maintain the Datacenter Business Continuity Plan for the continued operations of critical processes and required resources in the event of a disruption at least annually. The 'Business Continuity Management Exercise and Test Program Framework' document establishes the basis and process for exercising and testing of the plans for continuity and resumption of critical datacenter processes. **IM - 1.** An incident management framework with defined processes, roles, and responsibilities for the detection, escalation and response of incidents, has been established and communicated. **SOC2 - 4.** 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. **SOC2 - 15.** Azure has established baselines for OS deployments. Azure employs mechanisms to re-image production servers with the latest baseline configurations at least once a month or detect and troubleshoot exceptions or deviations from the baseline configuration in the production environment. The Azure OS and component teams review and update configuration settings and baseline configurations at least annually. **SOC2 - 18.** Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements for each information system	

Trust Criteria	Azure Activity	Test Result
	and the organization, should be explicitly defined, documented, and kept up to date. **SOC2 - 19.** A compliance program is managed with representation from various cross-functional teams and external parties to identify and manage compliance with relevant statutory, regulatory and contractual requirements. **SOC2 - 20.** Azure performs periodic Information Security Management System (ISMS) reviews and reviews results 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. Audit activities are planned and agreed upon in advance by stakeholders and any access required to perform the audits requires approval. **SOC2 - 25.** Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within the Azure environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Corporate, External, and Legal Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements. **SOC2 - 26.** Microsoft Azure 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. **VM - 1.** Azure platform components are configured to log and collect security events. **VM - 2.** Administrator activity in the Azure platform is logged. **VM - 3.** A monitoring system to monitor the Azure platform for potential malicious activity and intrusion past service trust boundaries has been implemented.	

Trust Criteria	Azure Activity	Test Result
	VM - 6. Procedures to monitor the Azure platform components for known security vulnerabilities have been established. Identified security vulnerabilities are remediated. **VM - 9.** Network devices in the scope boundary are configured to log and collect security events, and monitored for compliance with established security standards. **VM - 12.** The availability of Azure services is monitored through third-party and internal tools, and the status is communicated through a Service Dashboard. **DS - 18.** Microsoft performs a risk assessment for encryption and key management to evaluate changes and updates to cryptography controls.	
CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	**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. **BC - 1.** Business Continuity Plans (BCP) for critical Azure services, which provide roles and responsibilities and detailed procedures for recovery and reconstitution of systems to a known state per defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), have been documented and published. Plans are reviewed on an annual basis, at a minimum. **BC - 5.** Risk assessments are conducted to identify and assess business continuity risks related to Azure services. **BC - 7.** A Datacenter Business Continuity Management (BCM) program to respond to Microsoft's Enterprise Business Continuance Initiative has been implemented and includes documented procedures for mapping processes to pre-defined enterprise functions, establishing recovery strategies as well as developing and conducting test scenarios that enable the BCM program to mitigate risks and vulnerabilities and respond to major disruptive events.	**Exception noted:** **VM - 6:** Internal Audit of Microsoft identified multiple vulnerabilities associated with five in-scope services that were not remediated in a timely manner within the expected SLA. No additional exceptions were noted in our independent testing.

Trust Criteria	Azure Activity	Test Result
	BC - 8. A Datacenter Business Continuity Management Program defines business continuity planning and testing requirements for functions within the datacenters. Datacenters exercise, test and maintain the Datacenter Business Continuity Plan for the continued operations of critical processes and required resources in the event of a disruption at least annually. The ‘Business Continuity Management Exercise and Test Program Framework’ document establishes the basis and process for exercising and testing of the plans for continuity and resumption of critical datacenter processes. **IM - 1.** An incident management framework with defined processes, roles, and responsibilities for the detection, escalation and response of incidents, has been established and communicated. **SOC2 - 2.** Azure services maintain an automated inventory of key information assets. Automated quality control checks are implemented on all inventory data sources. **SOC2 - 15.** Azure has established baselines for OS deployments. Azure employs mechanisms to re-image production servers with the latest baseline configurations at least once a month or detect and troubleshoot exceptions or deviations from the baseline configuration in the production environment. The Azure OS and component teams review and update configuration settings and baseline configurations at least annually. **SOC2 - 18.** Relevant statutory, regulatory, and contractual requirements and the organization’s approach to meet these requirements for each information system and the organization, should be explicitly defined, documented, and kept up to date. **SOC2 - 19.** A compliance program is managed with representation from various cross-functional teams and external parties to identify and manage compliance with relevant statutory, regulatory and contractual requirements. **SOC2 - 20.** Azure performs periodic Information Security Management System (ISMS) reviews and reviews results with management. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by	

Trust Criteria	Azure Activity	Test Result
	reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions. Audit activities are planned and agreed upon in advance by stakeholders and any access required to perform the audits requires approval. **SOC2 - 25.** Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within the Azure environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Corporate, External, and Legal Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements. **SOC2 - 26.** Microsoft Azure 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. **VM - 1.** Azure platform components are configured to log and collect security events. **VM - 2.** Administrator activity in the Azure platform is logged. **VM - 3.** A monitoring system to monitor the Azure platform for potential malicious activity and intrusion past service trust boundaries has been implemented. **VM - 6.** Procedures to monitor the Azure platform components for known security vulnerabilities have been established. Identified security vulnerabilities are remediated. **VM - 9.** Network devices in the scope boundary are configured to log and collect security events, and monitored for compliance with established security standards. **VM - 12.** The availability of Azure services is monitored through third-party and internal tools, and the status is communicated through a Service Dashboard.	

Trust Criteria	Azure Activity	Test Result
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	**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. **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. **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. **BC - 5.** Risk assessments are conducted to identify and assess business continuity risks related to Azure services. **SOC2 - 4.** 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. **SOC2 - 18.** Relevant statutory, regulatory, and contractual requirements and the organization’s approach to meet these requirements for each information system and the organization, should be explicitly defined, documented, and kept up to date. **SOC2 - 19.** A compliance program is managed with representation from various cross-functional teams and external parties to identify and manage compliance with relevant statutory, regulatory and contractual requirements. **SOC2 - 20.** Azure performs periodic Information Security Management System (ISMS) reviews and reviews results 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.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	Audit activities are planned and agreed upon in advance by stakeholders and any access required to perform the audits requires approval. **SOC2 - 25.** Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within the Azure environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Corporate, External, and Legal Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements. **SOC2 - 26.** Microsoft Azure 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.	

MONITORING ACTIVITIES

Trust Criteria	Azure 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.	**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. **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. **SOC2 - 15.** Azure has established baselines for OS deployments. Azure employs mechanisms to re-image production servers with the latest baseline configurations at least once a month or detect and troubleshoot exceptions or deviations from the baseline configuration in the production	**Exception noted:** **VM - 6:** Internal Audit of Microsoft identified multiple vulnerabilities associated with five in-scope services that were not remediated in a timely manner within the expected SLA. No additional exceptions were noted in our independent testing.

Trust Criteria	Azure Activity	Test Result
	environment. The Azure OS and component teams review and update configuration settings and baseline configurations at least annually. **SOC2 - 20.** Azure performs periodic Information Security Management System (ISMS) reviews and reviews results 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. Audit activities are planned and agreed upon in advance by stakeholders and any access required to perform the audits requires approval. **SOC2 - 26.** Microsoft Azure 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. **SOC2 - 27.** Microsoft Azure undergoes independent audits and assessments, to monitor and verify compliance with security requirements, at least annually. Findings are recorded, reviewed, prioritized, and remediation plans are developed. **IM - 1.** An incident management framework with defined processes, roles, and responsibilities for the detection, escalation and response of incidents, has been established and communicated. **IM - 2.** Events, thresholds, and metrics have been defined and configured to detect incidents and alert the associated Operations team. **IM - 3.** The Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures. **VM - 3.** A monitoring system to monitor the Azure platform for potential malicious activity and intrusion past service trust boundaries has been implemented. **VM - 4.** Procedures to investigate and respond to malicious events detected by the Azure monitoring system in a timely manner have been established.	

Trust Criteria	Azure Activity	Test Result
	VM - 6. Procedures to monitor the Azure platform components for known security vulnerabilities have been established. Identified security vulnerabilities are remediated. **VM - 8.** Penetration testing of critical infrastructure components is performed at least annually based on documented Penetration testing procedures and findings are documented, tracked, and remediated. **VM - 9.** Network devices in the scope boundary are configured to log and collect security events, and monitored for compliance with established security standards. **VM - 10.** Azure provides logging mechanisms that can be configured by customers to log activities and performance metrics.	
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.	**ELC - 4.** The Audit Committee (AC) reviews its Charter and Responsibilities on an annual basis, as listed in its calendar. 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. **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. **SOC2 - 4.** 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. **SOC2 - 15.** Azure has established baselines for OS deployments. Azure employs mechanisms to re-image production servers with the latest baseline configurations at least once a month or detect and troubleshoot exceptions or deviations from the baseline configuration in the production environment. The Azure OS and component teams review and update configuration settings and baseline configurations at least annually.	**Exception noted:** **VM - 6:** Internal Audit of Microsoft identified multiple vulnerabilities associated with five in-scope services that were not remediated in a timely manner within the expected SLA. No additional exceptions were noted in our independent testing.

Trust Criteria	Azure Activity	Test Result
	SOC2 - 20. Azure performs periodic Information Security Management System (ISMS) reviews and reviews results 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. Audit activities are planned and agreed upon in advance by stakeholders and any access required to perform the audits requires approval. **SOC2 - 26.** Microsoft Azure 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. **IM - 1.** An incident management framework with defined processes, roles, and responsibilities for the detection, escalation and response of incidents, has been established and communicated. **IM - 2.** Events, thresholds, and metrics have been defined and configured to detect incidents and alert the associated Operations team. **IM - 3.** The Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures. **VM - 3.** A monitoring system to monitor the Azure platform for potential malicious activity and intrusion past service trust boundaries has been implemented. **VM - 4.** Procedures to investigate and respond to malicious events detected by the Azure monitoring system in a timely manner have been established. **VM - 6.** Procedures to monitor the Azure platform components for known security vulnerabilities have been established. Identified security vulnerabilities are remediated. **VM - 9.** Network devices in the scope boundary are configured to log and collect security events, and monitored for compliance with established security standards.	

Trust Criteria	Azure 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.	**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. **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. **BC - 4.** The BCP team conducts testing of the business continuity and disaster recovery plans established for Azure services, per the defined testing schedule for different loss scenario. Each loss scenario is tested at least annually. Issues identified during testing are resolved and plans are updated accordingly. **BC - 6.** Procedures for continuity of critical services provided by third-parties have been established. Contracts with third-parties are periodically monitored and reviewed for inconsistencies or non-conformance. Procedures to transition between critical third-parties based on results of monitoring are established. **CM - 2.** Secondary approval is required prior to all pull request check-ins to the production build, enforcing segregation among designated personal when implementing changes. **SOC2 - 20.** Azure performs periodic Information Security Management System (ISMS) reviews and reviews results 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. Audit activities are planned and agreed upon in advance by stakeholders and any access required to perform the audits requires approval. **SOC2 - 25.** Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within the Azure environment based on Microsoft's corporate procurement process. Designated	**Exception noted:** **CM - 2:** Management self-identified a vulnerability that could have allowed a single individual to submit and approve code bypassing SOD controls at the pull request level by using two user accounts owned by the same individual (i.e. Corp and Alt accounts). Management identified and disclosed 31 related instances from a large quantity of pull requests where developers self-approved their pull requests before checking them into the production build, leveraging multiple user accounts that they owned. Additionally, tested 15 change samples subsequent to September 30, 2024 and no additional exceptions were noted.

Trust Criteria	Azure Activity	Test Result
	responsibilities are defined to coordinate with relevant corporate groups (e.g., Corporate, External, and Legal Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements. **SOC2 - 26.** Microsoft Azure 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. **SDL - 3.** Responsibilities for submitting and approving production deployments are segregated within the Azure teams.	
CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	**BC - 4.** The BCP team conducts testing of the business continuity and disaster recovery plans established for Azure services, per the defined testing schedule for different loss scenario. Each loss scenario is tested at least annually. Issues identified during testing are resolved and plans are updated accordingly. **BC - 6.** Procedures for continuity of critical services provided by third-parties have been established. Contracts with third-parties are periodically monitored and reviewed for inconsistencies or non-conformance. Procedures to transition between critical third-parties based on results of monitoring are established. **OA - 1.** Administrative access to the Service environment is controlled through defined interfaces that require authentication using appropriate credentials. Privileges (i.e., read, write) are restricted to authorized personnel through designated channels based on job responsibilities. **OA - 2.** Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning employee, contractor, and service provider access to specific applications or information resources. **OA - 3.** Procedures are in place to disable accounts on a timely basis, upon the user's termination. **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. **OA - 10.** Users are granted access to network devices in the scope boundary upon receiving appropriate approvals.	**Exception noted:** **SDL - 1:** For 15 of the 36 sampled services, SDL review was not completed within the annual cadence. For the period 04/01/2024 to 08/31/2024, Internal Audit of Microsoft identified one additional sample that did not meet the annual SDL review cadence. Additionally, Internal Audit of Microsoft identified one sampled service in which two exceptions were not approved timely and by the appropriate personnel as per Microsoft's SDL Methodology.

Trust Criteria	Azure Activity	Test Result
	OA - 21. Access to production resources requires the use of a Secure Admin Workstation (SAW) which requires MFA for access. **SOC2 - 20.** Azure performs periodic Information Security Management System (ISMS) reviews and reviews results 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. Audit activities are planned and agreed upon in advance by stakeholders and any access required to perform the audits requires approval. **SOC2 - 25.** Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within the Azure environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Corporate, External, and Legal Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements. **SOC2 - 26.** Microsoft Azure 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. **SDL - 1.** Development of new features and changes to the Azure services follow a defined approach based on the Microsoft Security Development Lifecycle (SDL) methodology. The SDL review for each service is performed on an annual basis. **SDL - 2.** Applicable operational security and internal control requirements are documented, and implemented for Azure services based on Microsoft SDL methodology.	
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.	**ELC - 2.** Microsoft Compliance & 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 & 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.	No exceptions noted.

Trust Criteria	Azure 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. **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. **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. **IS - 1.** A security policy that defines the information security rules and requirements for the Service environment has been established and communicated. **IS - 2.** The Security Policy is reviewed and approved annually by appropriate management. **IS - 3.** Management has established defined roles and responsibilities to oversee implementation of the Security Policy across Azure. **IS - 4.** An information security education and awareness program that includes policy training and periodic security updates for Azure personnel has been established. **IM - 3.** The Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures. **VM - 4.** Procedures to investigate and respond to malicious events detected by the Azure monitoring system in a timely manner have been established.	

Trust Criteria	Azure 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.	**DS - 3.** Internal communication between key Azure components where customer data is transmitted / involved is secured using encryption. **DS - 9.** Backup restoration procedures are defined and backup data integrity checks are performed through standard restoration activities. **DS - 10.** Guidelines for the disposal of storage media have been established. **DS - 11.** Data corresponding to Azure is backed up to another region other than the primary data location and retained as per the retention policy. **DS - 15.** Customer data is retained and removed per the defined terms within the Product Terms, when a customer's subscription expires, or is terminated. **DS - 16.** Each Online Service's customer's data is segregated from other Online Services' customers' data, either logically or physically. **ED - 1.** Production servers that reside in edge locations are encrypted at the drive level. **ED - 3.** All unused IO ports on production servers that reside in edge locations are disabled through the configuration settings at the OS-level. **LA - 1.** External access to Azure services and the customer data stored in the service requires authentication and is restricted based on customer configured authorization settings. **LA - 2.** Customer credentials used to access Azure services meet the applicable password policy requirements. Temporary credentials assigned to users by the service expire within 14 days and users are forced to change these credentials when using them for the first time. **LA - 3.** Logical segregation to restrict unauthorized access to other customer tenants is implemented. **LA - 4.** Customer data that is designated as "confidential" is protected while in storage within Azure services.	**Exception noted:** **DS - 9:** Management identified a vulnerability in the supporting third-party software used in scheduling of their internal offline backups. As a result, management paused backups, resulting in the control not operating effectively from February 22, 2025. **DS - 11:** Management identified a vulnerability in the supporting third-party software used in scheduling of their internal offline backups. As a result, management paused backups, resulting in the control not operating effectively from February 22, 2025.

Trust Criteria	Azure Activity	Test Result
	LA - 5. User sessions within Azure can be configured by customers to expire after a stipulated period of inactivity. **LA - 9.** Service initializes the resource groups within the management portal based on the customer configured templates. Service allows customers to monitor and control the distribution of system resources created within the resource group in order to prevent resources from being congested. **LA - 11.** One Time Passwords (OTPs) used for self-service password reset are randomly generated. OTPs expire after a pre-defined time limit. OTPs sent to the customer administrator are required to be validated before a password change is allowed. SSPR does not display user identifiable information during the password reset. Microsoft Entra ID password policy requirements are enforced on the new passwords supplied by customer administrators within SSPR portal. New passwords supplied by customer administrators are protected during transmission over external networks. **LA - 12.** Images may be customized and access to images may be restricted by the customer. Updates to available images are communicated to through customer-facing websites. **OA - 1.** Administrative access to the Service environment is controlled through defined interfaces that require authentication using appropriate credentials. Privileges (i.e., read, write) are restricted to authorized personnel through designated channels based on job responsibilities. **OA - 2.** Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning employee, contractor, and service provider access to specific applications or information resources. **OA - 3.** Procedures are in place to disable accounts on a timely basis, upon the user's termination. **OA - 4.** User credentials adhere to established corporate standards and group policies for password requirements: - expiration - length - complexity	

Trust Criteria	Azure Activity	Test Result
	- history Initial passwords have secure mechanisms in place for distribution and first-time use. For production domains where passwords are not in use, multi-factor authentication is 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. **OA - 6.** Production domain-level user accounts are disabled after 90 days of inactivity. **OA - 7.** Procedures for granting Azure personnel temporary access to customer data and applications, upon appropriate approval for customer support or incident handling purposes, have been established. **OA - 8.** Authentication over an encrypted Remote Desktop Connection is used for administrator access to the production environment. **OA - 9.** User groups and Access Control Lists have been established to restrict access to network devices in the scope boundary. **OA - 10.** Users are granted access to network devices in the scope boundary upon receiving appropriate approvals. **OA - 13.** Access to network devices in the scope boundary is restricted through a limited number of entry points that require authentication over an encrypted connection. **OA - 14.** Access to network devices in the scope boundary requires two-factor authentication and / or other secure mechanisms. **OA - 15.** Passwords used to access Azure network devices are restricted to authorized individuals based on job responsibilities and changed on a periodic basis. **OA - 16.** Network filtering to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted service components is implemented.	

Trust Criteria	Azure Activity	Test Result
	OA - 18. Azure network is segregated to separate customer traffic from management traffic. **OA - 20.** Alerts are generated when a break-glass account is used to access a production subscription. **OA - 21.** Access to production resources requires the use of a Secure Admin Workstation (SAW) which requires MFA for access. **SOC2 - 1.** Azure assets are classified in accordance with Microsoft Online Services Classification Guidelines. The classification is documented, reviewed, and approved by the authorizing official. **SOC2 - 2.** Azure services maintain an automated inventory of key information assets. Automated quality control checks are implemented on all inventory data sources.	
CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	**LA - 1.** External access to Azure services and the customer data stored in the service requires authentication and is restricted based on customer configured authorization settings. **LA - 11.** One Time Passwords (OTPs) used for self-service password reset are randomly generated. OTPs expire after a pre-defined time limit. OTPs sent to the customer administrator are required to be validated before a password change is allowed. SSPR does not display user identifiable information during the password reset. Microsoft Entra ID password policy requirements are enforced on the new passwords supplied by customer administrators within SSPR portal. New passwords supplied by customer administrators are protected during transmission over external networks. **OA - 1.** Administrative access to the Service environment is controlled through defined interfaces that require authentication using appropriate credentials. Privileges (i.e., read, write) are restricted to authorized personnel through designated channels based on job responsibilities. **OA - 2.** Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning employee, contractor, and service provider access to specific applications or information resources.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	OA - 3. Procedures are in place to disable accounts on a timely basis, upon the user's termination. **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. **OA - 6.** Production domain-level user accounts are disabled after 90 days of inactivity. **OA - 7.** Procedures for granting Azure personnel temporary access to customer data and applications, upon appropriate approval for customer support or incident handling purposes, have been established. **OA - 10.** Users are granted access to network devices in the scope boundary upon receiving appropriate approvals. **OA - 13.** Access to network devices in the scope boundary is restricted through a limited number of entry points that require authentication over an encrypted connection. **OA - 14.** Access to network devices in the scope boundary requires two-factor authentication and / or other secure mechanisms.	
CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	**LA - 11.** One Time Passwords (OTPs) used for self-service password reset are randomly generated. OTPs expire after a pre-defined time limit. OTPs sent to the customer administrator are required to be validated before a password change is allowed. SSPR does not display user identifiable information during the password reset. Microsoft Entra ID password policy requirements are enforced on the new passwords supplied by customer administrators within SSPR portal. New passwords supplied by customer administrators are protected during transmission over external networks. **OA - 1.** Administrative access to the Service environment is controlled through defined interfaces that require authentication using appropriate credentials. Privileges (i.e., read, write) are restricted to authorized personnel through designated channels based on job responsibilities.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	OA - 2. Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning employee, contractor, and service provider access to specific applications or information resources. **OA - 3.** Procedures are in place to disable accounts on a timely basis, upon the user's termination. **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. **OA - 6.** Production domain-level user accounts are disabled after 90 days of inactivity. **OA - 7.** Procedures for granting Azure personnel temporary access to customer data and applications, upon appropriate approval for customer support or incident handling purposes, have been established. **OA - 8.** Authentication over an encrypted Remote Desktop Connection is used for administrator access to the production environment. **OA - 9.** User groups and Access Control Lists have been established to restrict access to network devices in the scope boundary. **OA - 10.** Users are granted access to network devices in the scope boundary upon receiving appropriate approvals. **OA - 14.** Access to network devices in the scope boundary requires two-factor authentication and / or other secure mechanisms. **OA - 15.** Passwords used to access Azure network devices are restricted to authorized individuals based on job responsibilities and changed on a periodic basis. **OA - 16.** Network filtering to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted service components is implemented.	
CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up	**PE - 1.** Procedures to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors, have been established.	**Exception noted:** **PE - 4:**

Trust Criteria	Azure Activity	Test Result
media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	**PE - 2.** Security verification and check-in for personnel requiring temporary access to the interior of the datacenter facility, including tour groups or visitors, are required. **PE - 3.** Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team. **PE - 4.** Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals. **PE - 5.** The datacenter facility is monitored 24x7 by security personnel.	For 1 of 17 sampled datacenters, while there are various layers of physical access mechanisms that were determined to be properly implemented, two instances of physical access mechanisms were not properly administered: - A trash door that provides access to the loading area was not fully closed. - While keycards were required to enter the generator area, several generator enclosures within the area that are normally secured with temporary-use physical keys had broken or unsecured locks. **PE - 5:** For 1 of the 32 sampled cameras, the tapes were not retained in accordance with the documented operating procedures.

Trust Criteria	Azure Activity	Test Result
CC6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	**DS - 10.** Guidelines for the disposal of storage media have been established. **PE - 1.** Procedures to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors, have been established. **PE - 2.** Security verification and check-in for personnel requiring temporary access to the interior of the datacenter facility, including tour groups or visitors, are required. **PE - 3.** Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team. **PE - 4.** Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals. **PE - 5.** The datacenter facility is monitored 24x7 by security personnel. **SOC2 - 3.** Datacenter team controls the delivery and removal of information system components through tickets on the Global Datacenter Operations (GDCO) ticketing system. Delivery and removal of information system components is authorized by system owners. System components / assets are tracked in the GDCO ticketing database.	**Exception noted:** **PE - 4:** For 1 of 17 sampled datacenters, while there are various layers of physical access mechanisms that were determined to be properly implemented, two instances of physical access mechanisms were not properly administered: - A trash door that provides access to the loading area was not fully closed. - While keycards were required to enter the generator area, several generator enclosures within the area that are normally secured with temporary-use physical keys had broken or unsecured locks. **PE - 5:** For 1 of the 32 sampled cameras, the tapes were not retained in accordance with the

Trust Criteria	Azure Activity	Test Result
		documented operating procedures.
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	**DS - 1.** Cryptographic certificates, keys, and customer access keys used for communication between Azure services and other internal components are stored securely and are rotated on a periodic basis. **DS - 2.** Customer data communicated through Azure service interfaces is encrypted during transmission over external networks. Location-aware technologies are implemented within the Azure portal to identify and validate authentication sessions. **DS - 3.** Internal communication between key Azure components where customer data is transmitted / involved is secured using encryption. **DS - 4.** Cryptographic controls are used for information protection within the Azure platform based on the Azure Cryptographic Policy and Key Management procedures. The policies and procedures include the key rotation, archival and deactivation processes. Keys must have identifiable owners (binding keys to identities) and key management policies. **DS - 10.** Guidelines for the disposal of storage media have been established. **DS - 13.** Production data on backup media is encrypted. **DS - 16.** Each Online Service's customer's data is segregated from other Online Services' customers' data, either logically or physically. **DS - 17.** Azure provides customers the ability to manage their own data encryption keys. **ED - 1.** Production servers that reside in edge locations are encrypted at the drive level. **ED - 3.** All unused IO ports on production servers that reside in edge locations are disabled through the configuration settings at the OS-level.	**Exception noted:** **DS - 1:** Three of 24 sampled secrets tested during the period 4/1/2024 to 12/31/2024 were not rotated as per the secret rotation cadence defined in the documented procedures. Further, tested 11 sampled secrets subsequent to December 31, 2024, and no additional exceptions were noted. Additionally, certain internal Microsoft platform keys were not rotated according to the prescribed cadence outlined in the internal policy. As mitigation, these keys were protected through other security practices, including additional encryption. Separately, as part of its investigation into the actions of Midnight

Trust Criteria	Azure Activity	Test Result
	LA - 1. External access to Azure services and the customer data stored in the service requires authentication and is restricted based on customer configured authorization settings. **LA - 2.** Customer credentials used to access Azure services meet the applicable password policy requirements. Temporary credentials assigned to users by the service expire within 14 days and users are forced to change these credentials when using them for the first time. **LA - 11.** One Time Passwords (OTPs) used for self-service password reset are randomly generated. OTPs expire after a pre-defined time limit. OTPs sent to the customer administrator are required to be validated before a password change is allowed. SSPR does not display user identifiable information during the password reset. Microsoft Entra ID password policy requirements are enforced on the new passwords supplied by customer administrators within SSPR portal. New passwords supplied by customer administrators are protected during transmission over external networks. **OA - 1.** Administrative access to the Service environment is controlled through defined interfaces that require authentication using appropriate credentials. Privileges (i.e., read, write) are restricted to authorized personnel through designated channels based on job responsibilities. **OA - 8.** Authentication over an encrypted Remote Desktop Connection is used for administrator access to the production environment. **OA - 13.** Access to network devices in the scope boundary is restricted through a limited number of entry points that require authentication over an encrypted connection. **OA - 14.** Access to network devices in the scope boundary requires two-factor authentication and / or other secure mechanisms. **OA - 16.** Network filtering to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted service components is implemented. **OA - 17.** External traffic to the customer VM(s) is restricted to customer - enabled ports and protocols.	Blizzard, Microsoft identified passwords and secrets impacting certain in-scope Azure services that were accessed by the threat actors through code repositories or Microsoft corporate email. Furthermore, Internal Audit of Microsoft identified multiple secrets associated with four in-scope services that were not rotated during the past year.

Trust Criteria	Azure Activity	Test Result
	PI - 3. Microsoft Azure performs input validation to restrict any non-permissible requests to the API. **VM - 7.** Procedures to configure and monitor network devices in the scope boundary, and resolve issues, have been established. **VM - 9.** Network devices in the scope boundary are configured to log and collect security events, and monitored for compliance with established security standards.	
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.	**DS - 2.** Customer data communicated through Azure service interfaces is encrypted during transmission over external networks. Location-aware technologies are implemented within the Azure portal to identify and validate authentication sessions. **DS - 3.** Internal communication between key Azure components where customer data is transmitted / involved is secured using encryption. **DS - 4.** Cryptographic controls are used for information protection within the Azure platform based on the Azure Cryptographic Policy and Key Management procedures. The policies and procedures include the key rotation, archival and deactivation processes. Keys must have identifiable owners (binding keys to identities) and key management policies. **DS - 10.** Guidelines for the disposal of storage media have been established. **DS - 13.** Production data on backup media is encrypted. **OA - 8.** Authentication over an encrypted Remote Desktop Connection is used for administrator access to the production environment. **OA - 13.** Access to network devices in the scope boundary is restricted through a limited number of entry points that require authentication over an encrypted connection. **OA - 14.** Access to network devices in the scope boundary requires two-factor authentication and / or other secure mechanisms.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
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.	**ED - 2.** Intrusion alerts are sent to the operator when physical access to the production servers that reside in edge locations is detected. **ED - 3.** All unused IO ports on production servers that reside in edge locations are disabled through the configuration settings at the OS-level. **CM - 1.** Procedures for managing different types of changes, including emergency changes, to the Azure platform have been documented and communicated. **CM - 6.** Procedures to manage changes to network devices in the scope boundary have been established. **CM - 9.** Datacenter change requests are classified, documented, and approved by the Operations Management Team. **CM - 12.** Azure has implemented tools to perform integrity verification checks to detect unauthorized changes to software, firmware and information. **IM - 1.** An incident management framework with defined processes, roles, and responsibilities for the detection, escalation and response of incidents, has been established and communicated. **OA - 1.** Administrative access to the Service environment is controlled through defined interfaces that require authentication using appropriate credentials. Privileges (i.e., read, write) are restricted to authorized personnel through designated channels based on job responsibilities. **OA - 2.** Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning employee, contractor, and service provider access to specific applications or information resources. **OA - 13.** Access to network devices in the scope boundary is restricted through a limited number of entry points that require authentication over an encrypted connection. **OA - 14.** Access to network devices in the scope boundary requires two-factor authentication and / or other secure mechanisms.	**Exception noted:** **CM - 12:** For the period April 1, 2024 to March 31, 2025, Internal Audit Team of Microsoft noted that code-signing was not configured for seven of the build pipelines associated with five of the in-scope services. No additional exceptions were noted in our independent testing. **VM - 6:** Internal Audit of Microsoft identified multiple vulnerabilities associated with five in-scope services that were not remediated in a timely manner within the expected SLA. No additional exceptions were noted in our independent testing.

Trust Criteria	Azure Activity	Test Result
	OA - 20. Alerts are generated when a break-glass account is used to access a production subscription. **PI - 3.** Microsoft Azure performs input validation to restrict any non-permissible requests to the API. **SOC2 - 15.** Azure has established baselines for OS deployments. Azure employs mechanisms to re-image production servers with the latest baseline configurations at least once a month or detect and troubleshoot exceptions or deviations from the baseline configuration in the production environment. The Azure OS and component teams review and update configuration settings and baseline configurations at least annually. **VM - 1.** Azure platform components are configured to log and collect security events. **VM - 2.** Administrator activity in the Azure platform is logged. **VM - 3.** A monitoring system to monitor the Azure platform for potential malicious activity and intrusion past service trust boundaries has been implemented. **VM - 4.** Procedures to investigate and respond to malicious events detected by the Azure monitoring system in a timely manner have been established. **VM - 5.** Procedures to evaluate and implement Microsoft-released patches to Service components have been established. **VM - 6.** Procedures to monitor the Azure platform components for known security vulnerabilities have been established. Identified security vulnerabilities are remediated. **VM - 7.** Procedures to configure and monitor network devices in the scope boundary, and resolve issues, have been established. **VM - 9.** Network devices in the scope boundary are configured to log and collect security events, and monitored for compliance with established security standards.	

Trust Criteria	Azure Activity	Test Result
	VM - 13. Vulnerabilities for network devices are evaluated and mitigated based on documented procedures.	

SYSTEM OPERATIONS

Trust Criteria	Azure Activity	Test Result
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.	**CM - 7.** Secure network configurations are applied and reviewed through defined change management procedures. **CM - 8.** The Technical Security Services team develops security configuration standards for systems in the physical environment that are consistent with industry-accepted hardening standards. These configurations are documented in system baselines, are reviewed annually, and relevant configuration changes are communicated to impacted teams. **CM - 12.** Azure has implemented tools to perform integrity verification checks to detect unauthorized changes to software, firmware and information. **ED - 1.** Production servers that reside in edge locations are encrypted at the drive level. **ED - 2.** Intrusion alerts are sent to the operator when physical access to the production servers that reside in edge locations is detected. **ED - 3.** All unused IO ports on production servers that reside in edge locations are disabled through the configuration settings at the OS-level. **PI - 3.** Microsoft Azure performs input validation to restrict any non-permissible requests to the API. **SOC2 - 15.** Azure has established baselines for OS deployments. Azure employs mechanisms to re-image production servers with the latest baseline configurations at least once a month or detect and troubleshoot exceptions or deviations from the baseline configuration in the production	**Exception noted:** **CM - 12:** For the period April 1, 2024 to March 31, 2025, Internal Audit Team of Microsoft noted that code-signing was not configured for seven of the build pipelines associated with five of the in-scope services. No additional exceptions were noted in our independent testing. **VM - 6:** Internal Audit of Microsoft identified multiple vulnerabilities associated with five in-scope services that were not remediated in a timely manner within the expected SLA.

Trust Criteria	Azure Activity	Test Result
	environment. The Azure OS and component teams review and update configuration settings and baseline configurations at least annually. **VM - 1.** Azure platform components are configured to log and collect security events. **VM - 2.** Administrator activity in the Azure platform is logged. **VM - 3.** A monitoring system to monitor the Azure platform for potential malicious activity and intrusion past service trust boundaries has been implemented. **VM - 4.** Procedures to investigate and respond to malicious events detected by the Azure monitoring system in a timely manner have been established. **VM - 5.** Procedures to evaluate and implement Microsoft-released patches to Service components have been established. **VM - 6.** Procedures to monitor the Azure platform components for known security vulnerabilities have been established. Identified security vulnerabilities are remediated. **VM - 7.** Procedures to configure and monitor network devices in the scope boundary, and resolve issues, have been established. **VM - 9.** Network devices in the scope boundary are configured to log and collect security events, and monitored for compliance with established security standards. **VM - 11.** Microsoft operating system updates for virtual machines are made available through Microsoft Security Response Center (MSRC) site and Windows Update. **VM - 13.** Vulnerabilities for network devices are evaluated and mitigated based on documented procedures.	No additional exceptions were noted in our independent testing.
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and	**BC - 9.** Datacenter Management teams conduct and document a resiliency assessment, specific to the datacenter's operations, on an annual basis or prior to proposed significant changes.	**Exception noted:** **CM - 12:**

Trust Criteria	Azure Activity	Test Result
errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	**CM - 12.** Azure has implemented tools to perform integrity verification checks to detect unauthorized changes to software, firmware and information. **DS - 5.** Backups of key Azure service components and secrets are performed regularly and stored in fault-tolerant (isolated) facilities. Backups are monitored and backup errors are investigated and followed-up on appropriately. **DS - 6.** Critical Azure components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services. **DS - 14.** Azure services are configured to automatically restore customer services upon detection of hardware and system failures. **ED - 1.** Production servers that reside in edge locations are encrypted at the drive level. **ED - 2.** Intrusion alerts are sent to the operator when physical access to the production servers that reside in edge locations is detected. **ED - 3.** All unused IO ports on production servers that reside in edge locations are disabled through the configuration settings at the OS-level. **IM - 1.** An incident management framework with defined processes, roles, and responsibilities for the detection, escalation and response of incidents, has been established and communicated. **IM - 3.** The Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures. **PE - 1.** Procedures to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors, have been established. **PE - 4.** Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals. **PE - 5.** The datacenter facility is monitored 24x7 by security personnel. **VM - 1.** Azure platform components are configured to log and collect security events.	For the period April 1, 2024 to March 31, 2025, Internal Audit Team of Microsoft noted that code-signing was not configured for seven of the build pipelines associated with five of the in-scope services. No additional exceptions were noted in our independent testing. **PE - 4:** For 1 of 17 sampled datacenters, while there are various layers of physical access mechanisms that were determined to be properly implemented, two instances of physical access mechanisms were not properly administered: - A trash door that provides access to the loading area was not fully closed. - While keycards were required to enter the generator area, several generator enclosures within the area that are normally secured with temporary-use physical

Trust Criteria	Azure Activity	Test Result
	VM - 2. Administrator activity in the Azure platform is logged. **VM - 3.** A monitoring system to monitor the Azure platform for potential malicious activity and intrusion past service trust boundaries has been implemented. **VM - 4.** Procedures to investigate and respond to malicious events detected by the Azure monitoring system in a timely manner have been established. **VM - 5.** Procedures to evaluate and implement Microsoft-released patches to Service components have been established. **VM - 6.** Procedures to monitor the Azure platform components for known security vulnerabilities have been established. Identified security vulnerabilities are remediated. **VM - 7.** Procedures to configure and monitor network devices in the scope boundary, and resolve issues, have been established. **VM - 9.** Network devices in the scope boundary are configured to log and collect security events, and monitored for compliance with established security standards. **VM - 10.** Azure provides logging mechanisms that can be configured by customers to log activities and performance metrics. **VM - 13.** Vulnerabilities for network devices are evaluated and mitigated based on documented procedures. **SOC2 - 15.** Azure has established baselines for OS deployments. Azure employs mechanisms to re-image production servers with the latest baseline configurations at least once a month or detect and troubleshoot exceptions or deviations from the baseline configuration in the production environment. The Azure OS and component teams review and update configuration settings and baseline configurations at least annually.	keys had broken or unsecured locks. **PE - 5:** For 1 of the 32 sampled cameras, the tapes were not retained in accordance with the documented operating procedures. **VM - 6:** Internal Audit of Microsoft identified multiple vulnerabilities associated with five in-scope services that were not remediated in a timely manner within the expected SLA. No additional exceptions were noted in our independent testing.
CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its	**ED - 2.** Intrusion alerts are sent to the operator when physical access to the production servers that reside in edge locations is detected.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
objectives (security incidents) and, if so, takes actions to prevent or address such failures.	**IM - 1.** An incident management framework with defined processes, roles, and responsibilities for the detection, escalation and response of incidents, has been established and communicated. **IM - 2.** Events, thresholds, and metrics have been defined and configured to detect incidents and alert the associated Operations team. **IM - 3.** The Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures. **IM - 4.** Incident post-mortem activities for severe incidents impacting the Azure environment are conducted. **IM - 5.** The Cyber Defense Operations Center (CDOC) team provides reports of information security events to Cloud + AI management on a quarterly basis. Problem statements for systemic issues are submitted to executive leadership for review. **IM - 6.** The Cyber Defense Operations Center (CDOC) team performs annual tests on the security incident response procedures. **PE - 8.** Datacenter physical security management reviews and approves the incident response procedures on a yearly basis. The incident security response procedures detail the appropriate steps to be taken in the event of a security incident and the methods to report security weaknesses. **SOC2 - 3.** Datacenter team controls the delivery and removal of information system components through tickets on the Global Datacenter Operations (GDCO) ticketing system. Delivery and removal of information system components is authorized by system owners. System components / assets are tracked in the GDCO ticketing database. **SOC2 - 6.** Azure maintains a Customer Support website that describes the process for customers and other external users to inform about potential security issues and submit complaints. Reported issues are reviewed and addressed per documented incident management procedures.	

Trust Criteria	Azure Activity	Test Result
	VM - 1. Azure platform components are configured to log and collect security events. **VM - 4.** Procedures to investigate and respond to malicious events detected by the Azure monitoring system in a timely manner have been established.	
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.	**ED - 2.** Intrusion alerts are sent to the operator when physical access to the production servers that reside in edge locations is detected. **IM - 1.** An incident management framework with defined processes, roles, and responsibilities for the detection, escalation and response of incidents, has been established and communicated. **IM - 2.** Events, thresholds, and metrics have been defined and configured to detect incidents and alert the associated Operations team. **IM - 3.** The Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures. **IM - 4.** Incident post-mortem activities for severe incidents impacting the Azure environment are conducted. **IM - 5.** The Cyber Defense Operations Center (CDOC) team provides reports of information security events to Cloud + AI management on a quarterly basis. Problem statements for systemic issues are submitted to executive leadership for review. **IM - 6.** The Cyber Defense Operations Center (CDOC) team performs annual tests on the security incident response procedures. **PE - 8.** Datacenter physical security management reviews and approves the incident response procedures on a yearly basis. The incident security response procedures detail the appropriate steps to be taken in the event of a security incident and the methods to report security weaknesses. **SOC2 - 3.** Datacenter team controls the delivery and removal of information system components through tickets on the Global Datacenter Operations (GDCO) ticketing system. Delivery and removal of information system components is	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	authorized by system owners. System components / assets are tracked in the GDCO ticketing database. **SOC2 - 6.** Azure maintains a Customer Support website that describes the process for customers and other external users to inform about potential security issues and submit complaints. Reported issues are reviewed and addressed per documented incident management procedures. **SOC2 - 9.** Azure maintains and notifies customers of potential changes and events that may impact security or availability of the services through an online Service Dashboard. Changes to the security commitments and security obligations of Azure customers are updated on the Azure website in a timely manner. **VM - 1.** Azure platform components are configured to log and collect security events. **VM - 4.** Procedures to investigate and respond to malicious events detected by the Azure monitoring system in a timely manner have been established. **VM - 12.** The availability of Azure services is monitored through third-party and internal tools, and the status is communicated through a Service Dashboard.	
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.	**BC - 4.** The BCP team conducts testing of the business continuity and disaster recovery plans established for Azure services, per the defined testing schedule for different loss scenario. Each loss scenario is tested at least annually. Issues identified during testing are resolved and plans are updated accordingly. **BC - 8.** A Datacenter Business Continuity Management Program defines business continuity planning and testing requirements for functions within the datacenters. Datacenters exercise, test and maintain the Datacenter Business Continuity Plan for the continued operations of critical processes and required resources in the event of a disruption at least annually. The 'Business Continuity Management Exercise and Test Program Framework' document establishes the basis and process for exercising and testing of the plans for continuity and resumption of critical datacenter processes.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	ED - 2. Intrusion alerts are sent to the operator when physical access to the production servers that reside in edge locations is detected. **IM - 1.** An incident management framework with defined processes, roles, and responsibilities for the detection, escalation and response of incidents, has been established and communicated. **IM - 2.** Events, thresholds, and metrics have been defined and configured to detect incidents and alert the associated Operations team. **IM - 3.** The Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures. **IM - 4.** Incident post-mortem activities for severe incidents impacting the Azure environment are conducted. **IM - 5.** The Cyber Defense Operations Center (CDOC) team provides reports of information security events to Cloud + AI management on a quarterly basis. Problem statements for systemic issues are submitted to executive leadership for review. **IM - 6.** The Cyber Defense Operations Center (CDOC) team performs annual tests on the security incident response procedures. **PE - 8.** Datacenter physical security management reviews and approves the incident response procedures on a yearly basis. The incident security response procedures detail the appropriate steps to be taken in the event of a security incident and the methods to report security weaknesses. **VM - 1.** Azure platform components are configured to log and collect security events. **VM - 4.** Procedures to investigate and respond to malicious events detected by the Azure monitoring system in a timely manner have been established. **VM - 5.** Procedures to evaluate and implement Microsoft-released patches to Service components have been established. **SOC2 - 3.** Datacenter team controls the delivery and removal of information system components through tickets on the Global Datacenter Operations (GDCO)	

Trust Criteria	Azure Activity	Test Result
	ticketing system. Delivery and removal of information system components is authorized by system owners. System components / assets are tracked in the GDCO ticketing database. **SOC2 - 6.** Azure maintains a Customer Support website that describes the process for customers and other external users to inform about potential security issues and submit complaints. Reported issues are reviewed and addressed per documented incident management procedures.	

CHANGE MANAGEMENT

Trust Criteria	Azure 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.	**CM - 1.** Procedures for managing different types of changes, including emergency changes, to the Azure platform have been documented and communicated. **CM - 2.** Secondary approval is required prior to all pull request check-ins to the production build, enforcing segregation among designated personal when implementing changes. **CM - 3.** Key stakeholders approve prior to deploying a release into production based on documented change management procedures. **CM - 4.** Software releases and configuration changes to the Azure platform are tested based on established criteria prior to production implementation. **CM - 5.** Implemented changes to the Azure platform 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. **CM - 6.** Procedures to manage changes to network devices in the scope boundary have been established. **CM - 7.** Secure network configurations are applied and reviewed through defined change management procedures.	**Exception noted:** **SDL - 1:** For 15 of the 36 sampled services, SDL review was not completed within the annual cadence. For the period 04/01/2024 to 08/31/2024, Internal Audit of Microsoft identified one additional sample that did not meet the annual SDL review cadence. Additionally, Internal Audit of Microsoft identified one sampled service in which two exceptions were not

Trust Criteria	Azure Activity	Test Result
	CM - 8. The Technical Security Services team develops security configuration standards for systems in the physical environment that are consistent with industry-accepted hardening standards. These configurations are documented in system baselines, are reviewed annually, and relevant configuration changes are communicated to impacted teams. **CM - 9.** Datacenter change requests are classified, documented, and approved by the Operations Management Team. **CM - 10.** Secure configurations for datacenter software are applied through defined change management procedures including documentation, testing and approval. **CM - 12.** Azure has implemented tools to perform integrity verification checks to detect unauthorized changes to software, firmware and information. **CM - 13.** Any changes to production via break-glass have been reviewed to ensure all changes were appropriate. Management monitors break-glass alerts on periodic basis to ensure that alerts are appropriately reviewed. **DS - 4.** Cryptographic controls are used for information protection within the Azure platform based on the Azure Cryptographic Policy and Key Management procedures. The policies and procedures include the key rotation, archival and deactivation processes. Keys must have identifiable owners (binding keys to identities) and key management policies. **IS - 1.** A security policy that defines the information security rules and requirements for the Service environment has been established and communicated. **LA - 4.** Customer data that is designated as “confidential” is protected while in storage within Azure services. **LA - 8.** The private root key belonging to the Azure services is protected from unauthorized access.	approved timely and by the appropriate personnel as per Microsoft's SDL Methodology. **CM - 2:** Management self-identified a vulnerability that could have allowed a single individual to submit and approve code bypassing SOD controls at the pull request level by using two user accounts owned by the same individual (i.e. Corp and Alt accounts). Management identified and disclosed 31 related instances from a large quantity of pull requests where developers self-approved their pull requests before checking them into the production build, leveraging multiple user accounts that they owned. Additionally, tested 15 change samples subsequent to September 30, 2024 and no additional exceptions were noted.

Trust Criteria	Azure Activity	Test Result
	SDL - 1. Development of new features and changes to the Azure services follow a defined approach based on the Microsoft Security Development Lifecycle (SDL) methodology. The SDL review for each service is performed on an annual basis. **SDL - 2.** Applicable operational security and internal control requirements are documented, and implemented for Azure services based on Microsoft SDL methodology. **SDL - 3.** Responsibilities for submitting and approving production deployments are segregated within the Azure teams. **SDL - 4.** New features and major changes are developed and tested in separate environments prior to production implementation. Production data is not replicated in test or development environments. **SDL - 5.** Azure Services use code repositories for managing source code changes. Procedures to approve code changes managed through source code repository are established. Code changes submitted to the repository are logged and can be traced to the individuals or system components executing them. **SDL - 6.** Source code builds are scanned for malware prior to release to production. **SOC2 - 1.** Azure assets are classified in accordance with Microsoft Online Services Classification Guidelines. The classification is documented, reviewed, and approved by the authorizing official. **SOC2 - 2.** Azure services maintain an automated inventory of key information assets. Automated quality control checks are implemented on all inventory data sources. **SOC2 - 15.** Azure has established baselines for OS deployments. Azure employs mechanisms to re-image production servers with the latest baseline configurations at least once a month or detect and troubleshoot exceptions or deviations from the baseline configuration in the production environment. The Azure OS and component teams review and update configuration settings and baseline configurations at least annually.	**CM - 12:** For the period April 1, 2024 to March 31, 2025, Internal Audit Team of Microsoft noted that code-signing was not configured for seven of the build pipelines associated with five of the in-scope services. No additional exceptions were noted in our independent testing.

Trust Criteria	Azure Activity	Test Result
	SOC2 - 19. A compliance program is managed with representation from various cross-functional teams and external parties to identify and manage compliance with relevant statutory, regulatory and contractual requirements. **SOC2 - 20.** Azure performs periodic Information Security Management System (ISMS) reviews and reviews results 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. Audit activities are planned and agreed upon in advance by stakeholders and any access required to perform the audits requires approval.	

RISK MITIGATION

Trust Criteria	Azure Activity	Test Result
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	**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. **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. **SOC2 - 20.** Azure performs periodic Information Security Management System (ISMS) reviews and reviews results 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. Audit activities are planned and agreed upon in advance by stakeholders and any access required to perform the audits requires approval.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	SOC2 - 26. Microsoft Azure 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.	
CC9.2 The entity assesses and manages risks associated with vendors and business partners.	**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. **BC - 6.** Procedures for continuity of critical services provided by third-parties have been established. Contracts with third-parties are periodically monitored and reviewed for inconsistencies or non-conformance. Procedures to transition between critical third-parties based on results of monitoring are established. **IS - 4.** An information security education and awareness program that includes policy training and periodic security updates for Azure personnel has been established. **SOC2 - 25.** Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within the Azure environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Corporate, External, and Legal Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements. **C5 - 2.** 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.	No exceptions noted.

ADDITIONAL CRITERIA FOR AVAILABILITY

Trust Criteria	Azure 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.	**BC - 3.** Azure has developed a Business Continuity and Disaster Recovery (BC / DR) Standard Operating Procedure and documentation that includes the defined information security and availability requirements. **BC - 7.** A Datacenter Business Continuity Management (BCM) program to respond to Microsoft's Enterprise Business Continuance Initiative has been implemented and includes documented procedures for mapping processes to pre-defined enterprise functions, establishing recovery strategies as well as developing and conducting test scenarios that enable the BCM program to mitigate risks and vulnerabilities and respond to major disruptive events. **BC - 8.** A Datacenter Business Continuity Management Program defines business continuity planning and testing requirements for functions within the datacenters. Datacenters exercise, test and maintain the Datacenter Business Continuity Plan for the continued operations of critical processes and required resources in the event of a disruption at least annually. The 'Business Continuity Management Exercise and Test Program Framework' document establishes the basis and process for exercising and testing of the plans for continuity and resumption of critical datacenter processes. **BC - 10.** The network is monitored to ensure availability and address capacity issues in a timely manner. **LA - 6.** The jobs configured by the customer administrators are executed within thirty (30) minutes of the scheduled job run and are repeated based on the defined recurrence settings. **LA - 7.** Quotas on Azure services are enforced as configured by the service administrators to protect against availability related issues. **LA - 10.** The errors generated during the job execution are monitored and appropriate action is taken based on the job settings defined by the customer administrator. **PI - 2.** Microsoft Azure management reviews portal performance monthly to evaluate compliance with customer SLA requirements.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	VM - 12. The availability of Azure services is monitored through third-party and internal tools, and the status is communicated through a Service Dashboard.	
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.	**BC - 3.** Azure has developed a Business Continuity and Disaster Recovery (BC / DR) Standard Operating Procedure and documentation that includes the defined information security and availability requirements. **BC - 4.** The BCP team conducts testing of the business continuity and disaster recovery plans established for Azure services, per the defined testing schedule for different loss scenario. Each loss scenario is tested at least annually. Issues identified during testing are resolved and plans are updated accordingly. **BC - 6.** Procedures for continuity of critical services provided by third-parties have been established. Contracts with third-parties are periodically monitored and reviewed for inconsistencies or non-conformance. Procedures to transition between critical third-parties based on results of monitoring are established. **BC - 7.** A Datacenter Business Continuity Management (BCM) program to respond to Microsoft's Enterprise Business Continuance Initiative has been implemented and includes documented procedures for mapping processes to pre-defined enterprise functions, establishing recovery strategies as well as developing and conducting test scenarios that enable the BCM program to mitigate risks and vulnerabilities and respond to major disruptive events. **BC - 8.** A Datacenter Business Continuity Management Program defines business continuity planning and testing requirements for functions within the datacenters. Datacenters exercise, test and maintain the Datacenter Business Continuity Plan for the continued operations of critical processes and required resources in the event of a disruption at least annually. The 'Business Continuity Management Exercise and Test Program Framework' document establishes the basis and process for exercising and testing of the plans for continuity and resumption of critical datacenter processes. **BC - 9.** Datacenter Management teams conduct and document a resiliency assessment, specific to the datacenter's operations, on an annual basis or prior to proposed significant changes.	**Exception noted:** **DS - 8:** Management identified a vulnerability in the supporting third-party software used in scheduling of their internal offline backups. As a result, management paused backups, resulting in the control not operating effectively from February 22, 2025. **DS - 9** Management identified a vulnerability in the supporting third-party software used in scheduling of their internal offline backups. As a result, management paused backups, resulting in the control not operating effectively from February 22, 2025. **DS - 11:** Management identified a vulnerability in the supporting third-party

Trust Criteria	Azure Activity	Test Result
	DS - 5. Backups of key Azure service components and secrets are performed regularly and stored in fault-tolerant (isolated) facilities. Backups are monitored and backup errors are investigated and followed-up on appropriately. **DS - 6.** Critical Azure components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services. **DS - 7.** Customer data is automatically replicated within Azure to minimize isolated faults. Customers are able to determine geographical regions of the data processing and storage, including data backups. **DS - 8.** Data Protection Services (DPS) backs up data for properties based on a defined schedule and upon request of the properties. Data is retained according to the data type identified by the property. DPS investigates backup errors and skipped files and follows up appropriately. **DS - 9.** Backup restoration procedures are defined and backup data integrity checks are performed through standard restoration activities. **DS - 11.** Data corresponding to Azure is backed up to another region other than the primary data location and retained as per the retention policy. **DS - 13.** Production data on backup media is encrypted. **DS - 14.** Azure services are configured to automatically restore customer services upon detection of hardware and system failures. **DS - 15.** Customer data is retained and removed per the defined terms within the Product Terms, when a customer’s subscription expires, or is terminated. **PE - 6.** Datacenter Management team maintains and tests datacenter-managed environmental equipment within the facility according to documented policy and maintenance procedures. **PE - 7.** Environmental controls have been implemented to protect systems inside datacenter facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.	software used in scheduling of their internal offline backups. As a result, management paused backups, resulting in the control not operating effectively from February 22, 2025.

Trust Criteria	Azure Activity	Test Result
A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.	**BC - 4.** The BCP team conducts testing of the business continuity and disaster recovery plans established for Azure services, per the defined testing schedule for different loss scenario. Each loss scenario is tested at least annually. Issues identified during testing are resolved and plans are updated accordingly. **BC - 8.** A Datacenter Business Continuity Management Program defines business continuity planning and testing requirements for functions within the datacenters. Datacenters exercise, test and maintain the Datacenter Business Continuity Plan for the continued operations of critical processes and required resources in the event of a disruption at least annually. The 'Business Continuity Management Exercise and Test Program Framework' document establishes the basis and process for exercising and testing of the plans for continuity and resumption of critical datacenter processes. **DS - 9.** Backup restoration procedures are defined and backup data integrity checks are performed through standard restoration activities.	**Exception noted:** **DS - 9:** Management identified a vulnerability in the supporting third-party software used in scheduling of their internal offline backups. As a result, management paused backups, resulting in the control not operating effectively from February 22, 2025.

ADDITIONAL CRITERIA FOR CONFIDENTIALITY

Trust Criteria	Azure Activity	Test Result
C1.1. The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	**DS - 10.** Guidelines for the disposal of storage media have been established. **DS - 15.** Customer data is retained and removed per the defined terms within the Product Terms, when a customer's subscription expires, or is terminated. **SOC2 - 1.** Azure assets are classified in accordance with Microsoft Online Services Classification Guidelines. The classification is documented, reviewed, and approved by the authorizing official. **SOC2 - 14.** Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information, should be identified and regularly reviewed.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
C1.2. The entity disposes of confidential information to meet the entity’s objectives related to confidentiality.	**DS - 10.** Guidelines for the disposal of storage media have been established. **DS - 15.** Customer data is retained and removed per the defined terms within the Product Terms, when a customer’s subscription expires, or is terminated.	No exceptions noted.

ADDITIONAL CRITERIA FOR PROCESSING INTEGRITY

Trust Criteria	Azure 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.	**DS - 15.** Customer data is retained and removed per the defined terms within the Product Terms, when a customer’s subscription expires, or is terminated. **OA - 19.** Microsoft Azure has published virtualization industry standards supported within its environment. **PI - 3.** Microsoft Azure performs input validation to restrict any non-permissible requests to the API. **SOC2 - 7.** Azure 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. **SOC2 - 8.** Azure maintains and distributes an accurate system description to authorized users. **SOC2 - 10.** Prior to engaging in Azure services, customers are required to review and agree with the acceptable use of data and the Azure service, as well as security and privacy requirements, which are defined in the Product Terms, Microsoft Online Subscription Agreement, Azure service Privacy Statement and Technical Overview of the Security Features in Azure service. **SOC2 - 28.** Customer data is accessible within agreed upon services in data formats compatible with providing those services.	No exceptions noted.

Trust Criteria	Azure 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.	**PI - 3.** Microsoft Azure performs input validation to restrict any non-permissible requests to the API. **PI - 4.** Microsoft Azure segregates and appropriately provisions the services based on request from customer through the portal / API.	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.	**CM - 1.** Procedures for managing different types of changes, including emergency changes, to the Azure platform have been documented and communicated. **CM - 4.** Software releases and configuration changes to the Azure platform are tested based on established criteria prior to production implementation. **CM - 5.** Implemented changes to the Azure platform 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. **CM - 6.** Procedures to manage changes to network devices in the scope boundary have been established. **DS - 5.** Backups of key Azure service components and secrets are performed regularly and stored in fault-tolerant (isolated) facilities. Backups are monitored and backup errors are investigated and followed-up on appropriately. **DS - 6.** Critical Azure components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services. **DS - 7.** Customer data is automatically replicated within Azure to minimize isolated faults. Customers are able to determine geographical regions of the data processing and storage, including data backups. **DS - 9.** Backup restoration procedures are defined and backup data integrity checks are performed through standard restoration activities. **DS - 14.** Azure services are configured to automatically restore customer services upon detection of hardware and system failures.	**Exception noted:** **DS - 9:** Management identified a vulnerability in the supporting third-party software used in scheduling of their internal offline backups. As a result, management paused backups, resulting in the control not operating effectively from February 22, 2025.

Trust Criteria	Azure Activity	Test Result
	ED - 1. Production servers that reside in edge locations are encrypted at the drive level. **ED - 2.** Intrusion alerts are sent to the operator when physical access to the production servers that reside in edge locations is detected. **ED - 3.** All unused IO ports on production servers that reside in edge locations are disabled through the configuration settings at the OS-level. **IM - 3.** The Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures. **LA - 10.** The errors generated during the job execution are monitored and appropriate action is taken based on the job settings defined by the customer administrator. **LA - 11.** One Time Passwords (OTPs) used for self-service password reset are randomly generated. OTPs expire after a pre-defined time limit. OTPs sent to the customer administrator are required to be validated before a password change is allowed. SSPR does not display user identifiable information during the password reset. Microsoft Entra ID password policy requirements are enforced on the new passwords supplied by customer administrators within SSPR portal. New passwords supplied by customer administrators are protected during transmission over external networks. **OA - 1.** Administrative access to the Service environment is controlled through defined interfaces that require authentication using appropriate credentials. Privileges (i.e., read, write) are restricted to authorized personnel through designated channels based on job responsibilities. **OA - 2.** Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning employee, contractor, and service provider access to specific applications or information resources. **OA - 7.** Procedures for granting Azure personnel temporary access to customer data and applications, upon appropriate approval for customer support or incident handling purposes, have been established.	

Trust Criteria	Azure Activity	Test Result
	OA - 13. Access to network devices in the scope boundary is restricted through a limited number of entry points that require authentication over an encrypted connection. **OA - 14.** Access to network devices in the scope boundary requires two-factor authentication and / or other secure mechanisms. **PE - 6.** Datacenter Management team maintains and tests datacenter-managed environmental equipment within the facility according to documented policy and maintenance procedures. **PI - 1.** Microsoft Azure monitors the transactions invoked by the customer and relays them appropriately to the suitable Resource Provider (RP) end-point. Actions are taken in response to defined threshold events. **PI - 2.** Microsoft Azure management reviews portal performance monthly to evaluate compliance with customer SLA requirements. **PI - 4.** Microsoft Azure segregates and appropriately provisions the services based on request from customer through the portal / API.	
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.	**CM - 1.** Procedures for managing different types of changes, including emergency changes, to the Azure platform have been documented and communicated. **CM - 4.** Software releases and configuration changes to the Azure platform are tested based on established criteria prior to production implementation. **CM - 5.** Implemented changes to the Azure platform 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. **CM - 6.** Procedures to manage changes to network devices in the scope boundary have been established. **CM - 12.** Azure has implemented tools to perform integrity verification checks to detect unauthorized changes to software, firmware and information.	**Exception noted:** **CM - 12:** For the period April 1, 2024 to March 31, 2025, Internal Audit Team of Microsoft noted that code-signing was not configured for seven of the build pipelines associated with five of the in-scope services. No additional exceptions were noted in our independent testing.

Trust Criteria	Azure Activity	Test Result
	DS - 16. Each Online Service’s customer’s data is segregated from other Online Services’ customers’ data, either logically or physically. **IM - 3.** The Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures. **LA - 3.** Logical segregation to restrict unauthorized access to other customer tenants is implemented. **PI - 4.** Microsoft Azure segregates and appropriately provisions the services based on request from customer through the portal / API.	
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.	**DS - 5.** Backups of key Azure service components and secrets are performed regularly and stored in fault-tolerant (isolated) facilities. Backups are monitored and backup errors are investigated and followed-up on appropriately. **DS - 6.** Critical Azure components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services. **DS - 9.** Backup restoration procedures are defined and backup data integrity checks are performed through standard restoration activities. **DS - 10.** Guidelines for the disposal of storage media have been established. **DS - 14.** Azure services are configured to automatically restore customer services upon detection of hardware and system failures. **DS - 15.** Customer data is retained and removed per the defined terms within the Product Terms, when a customer’s subscription expires, or is terminated.	**Exception noted:** **DS - 9:** Management identified a vulnerability in the supporting third-party software used in scheduling of their internal offline backups. As a result, management paused backups, resulting in the control not operating effectively from February 22, 2025.

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 Activity	Test Result
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. The measures for setting up, implementing, maintaining and continuously improving the ISMS are documented. The documentation includes: • 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).	**SOC2 - 20.** Azure performs periodic Information Security Management System (ISMS) reviews and reviews results 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. Audit activities are planned and agreed upon in advance by stakeholders and any access required to perform the audits requires approval. **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.	No exceptions noted.
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. The policy describes:	**IS - 1.** A security policy that defines the information security rules and requirements for the Service environment has been established and communicated. **IS - 2.** The Security Policy is reviewed and approved annually by appropriate management.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
• 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.	**IS - 3.** Management has established defined roles and responsibilities to oversee implementation of the Security Policy across Azure. **IS - 4.** An information security education and awareness program that includes policy training and periodic security updates for Azure personnel has been established.	
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: • Vulnerabilities; • Security incidents; and • Malfunctions. 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). The communication of changes to the interfaces and dependencies takes place in a	**IS - 3.** Management has established defined roles and responsibilities to oversee implementation of the Security Policy across Azure. **IM - 1.** An incident management framework with defined processes, roles, and responsibilities for the detection, escalation and response of incidents, has been established and communicated. **SOC2 - 6.** Azure maintains a Customer Support website that describes the process for customers and other external users to inform about potential security issues and submit complaints. Reported issues are reviewed and addressed per documented incident management procedures. **SOC2 - 7.** Azure 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. **SOC2 - 9.** Azure maintains and notifies customers of potential changes and events that may impact security or availability of the services through an online Service Dashboard. Changes to the security commitments and security obligations of Azure customers are updated on the Azure website in a timely manner.	No exceptions noted.

C5 Criteria	Azure 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 - 13.** Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees are provided Microsoft's Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage. Employees are required to acknowledge agreements to return Microsoft assets upon termination. **C5 - 12.** Azure has a shared responsibility model available on the trust center website describing the responsibilities between Azure and its customers.	
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. 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: • 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. If separation cannot be established for organisational or technical reasons, measures are in place to monitor the activities in order to detect unauthorised or	**SOC2 - 18.** Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements for each information system and the organization, should be explicitly defined, documented, and kept up to date. **SOC2 - 26.** Microsoft Azure 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. **OA - 20.** Alerts are generated when a break-glass account is used to access a production subscription. **CM - 1.** Procedures for managing different types of changes, including emergency changes, to the Azure platform have been documented and communicated. **CM - 2.** Secondary approval is required prior to all pull request check-ins to the production build, enforcing segregation among designated personal when implementing changes. **CM - 3.** Key stakeholders approve prior to deploying a release into production based on documented change management procedures. **CM - 4.** Software releases and configuration changes to the Azure platform are tested based on established criteria prior to production implementation. **CM - 12.** Azure has implemented tools to perform integrity verification checks to detect unauthorized changes to software, firmware and information.	**Exception noted.** **CM - 2:** Management self-identified a vulnerability that could have allowed a single individual to submit and approve code bypassing SOD controls at the pull request level by using two user accounts owned by the same individual (i.e. Corp and Alt accounts). Management identified and disclosed 31 related instances from a large quantity of pull requests where developers self-approved their pull requests before checking them into the production build, leveraging multiple user accounts that they owned.

C5 Criteria	Azure Activity	Test Result
unintended changes as well as misuse and to take appropriate actions.	**CM - 13.** Any changes to production via break-glass have been reviewed to ensure all changes were appropriate. Management monitors break-glass alerts on periodic basis to ensure that alerts are appropriately reviewed. **SDL - 3.** Responsibilities for submitting and approving production deployments are segregated within the Azure teams. **PI - 4.** Microsoft Azure segregates and appropriately provisions the services based on request from customer through the portal / API. **DS - 18.** Microsoft performs a risk assessment for encryption and key management to evaluate changes and updates to cryptography controls.	Additionally, tested 15 change samples subsequent to September 30, 2024 and no additional exceptions were noted. **CM - 12:** For the period April 1, 2024 to March 31, 2025, Internal Audit Team of Microsoft noted that code-signing was not configured for seven of the build pipelines associated with five of the in-scope services. No additional exceptions were noted in our independent testing.
OIS-05 The Cloud Service Provider leverages relevant authorities and interest 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).	**SOC2 - 18.** Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements for each information system and the organization, should be explicitly defined, documented, and kept up to date. **SOC2 - 19.** A compliance program is managed with representation from various cross-functional teams and external parties to identify and manage compliance with relevant statutory, regulatory and contractual requirements.	No exceptions noted.
OIS-06 Policies and instructions for risk management procedures are documented, communicated and provided in accordance with SP-01 for the following aspects:	**SOC2 - 25.** Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within the Azure environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g.,	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
• 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 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.	Corporate, External, and Legal Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements. **SOC2 - 26.** Microsoft Azure 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. **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. **DS - 18.** Microsoft performs a risk assessment for encryption and key management to evaluate changes and updates to cryptography controls.	
OIS-07 The Cloud Service Provider executes the process for handling risks as needed or 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: • Processing, storage or transmission of data of cloud customers with different protection needs;	**SOC2 - 25.** Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within the Azure environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Corporate, External, and Legal Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements. **SOC2 - 26.** Microsoft Azure 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. **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	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
• 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. 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.	acceptable thresholds are reported to the Board of Directors on behalf of senior management. **C5 - 12.** Azure has a shared responsibility model available on the trust center website describing the responsibilities between Azure and its customers.	

SP: Security Policies and Instructions

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

C5 Criteria	Azure Activity	Test Result
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	**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.** A security policy that defines the information security rules and requirements for the Service environment has been established and communicated.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
The policies and instructions are version controlled and approved by the top management of the Cloud Service Provider or an authorised body The policies and instructions describe at least the following aspects: • 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.	**IS - 2.** The Security Policy is reviewed and approved annually by appropriate management. **IS - 3.** Management has established defined roles and responsibilities to oversee implementation of the Security Policy across Azure. **IS - 4.** An information security education and awareness program that includes policy training and periodic security updates for Azure personnel has been established. **SOC2 - 18.** Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements for each information system and the organization, should be explicitly defined, documented, and kept up to date.	
SP-02. Information security policies and instructions are reviewed at least annually for adequacy by the Cloud Service Provider's subject matter experts. The review shall consider at least the following aspects: • Organisational and technical changes in the procedures for providing the cloud service; and	**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 - 2.** The Security Policy is reviewed and approved annually by appropriate management. **SOC2 - 18.** Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements for each information system and the organization, should be explicitly defined, documented, and kept up to date.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
• Legal and regulatory changes in the Cloud Service Provider's environment. Revised policies and instructions are approved before they become effective.	**SOC2 - 20.** Azure performs periodic Information Security Management System (ISMS) reviews and reviews results 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. Audit activities are planned and agreed upon in advance by stakeholders and any access required to perform the audits requires approval.	
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.	**SOC2 - 4.** 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. **SOC2 - 25.** Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within the Azure environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Corporate, External, and Legal Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements. **SOC2 - 26.** Microsoft Azure 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.	No exceptions noted.

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 Activity	Test Result
HR-01 The competency and integrity of all internal and external employees of the Cloud	**SOC2 - 12.** Microsoft personnel and contingent staff undergo formal screening, including background verification checks, as a part of the hiring process prior to	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
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. To the extent permitted by law, the review will cover the following areas: • Verification of the person through identity card; • Verification of the CV; • Verification of academic titles and degrees; • Request of a police clearance certificate for applicants; • Certificate of good conduct or national equivalent; and • Evaluation of the risk to be blackmailed.	being granted access. Additional screening is conducted in accordance with customer specific requirements, for employees with access to applicable data.	
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. 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	**SOC2 - 13.** Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees are provided Microsoft’s Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage. Employees are required to acknowledge agreements to return Microsoft assets upon termination. **SOC2 - 14.** Requirements for confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information, should be identified and regularly reviewed.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
customer data or system components under the responsibility of the Cloud Service Provider used to provide the cloud service in the production environment.		
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: • 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.	**IS - 4.** An information security education and awareness program that includes policy training and periodic security updates for Azure personnel has been established. **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.	No exceptions noted.
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:	**SOC2 - 11.** Microsoft has defined disciplinary actions for employees and contingent staff that commit a security breach or violate Microsoft Security Policy.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
• Verifying whether a violation has occurred; and • Consideration of the nature and severity of the violation and its impact. The internal and external employees of the Cloud Service Provider are informed about possible disciplinary measures. The use of disciplinary measures is appropriately documented.		
HR-05 Internal and external employees have been informed about which 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.	**SOC2 - 13.** Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees are provided Microsoft's Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage. Employees are required to acknowledge agreements to return Microsoft assets upon termination. **SOC2 - 14.** Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information, should be identified and regularly reviewed.	No exceptions noted.
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. 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	**SOC2 - 7.** Azure 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. **SOC2 - 9.** Azure maintains and notifies customers of potential changes and events that may impact security or availability of the services through an online Service Dashboard. Changes to the security commitments and security obligations of Azure customers are updated on the Azure website in a timely manner. **SOC2 - 13.** Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
the Cloud Service Provider before authorisation to access data of cloud customers is granted. 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. 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.	hire. In addition, employees are provided Microsoft's Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage. Employees are required to acknowledge agreements to return Microsoft assets upon termination. **SOC2 - 14.** Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information, should be identified and regularly reviewed. **SOC2 - 25.** Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within the Azure environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Corporate, External, and Legal Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements.	

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 Activity	Test Result
AM-01 The Cloud Service Provider has established procedures for inventorying assets. 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.	**SOC2 - 1.** Azure assets are classified in accordance with Microsoft Online Services Classification Guidelines. The classification is documented, reviewed, and approved by the authorizing official. **SOC2 - 2.** Azure services maintain an automated inventory of key information assets. Automated quality control checks are implemented on all inventory data sources.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
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.		
AM-02 Policies and instructions for acceptable use and safe handling of assets are documented, communicated and provided in accordance with SP-01 and address the following aspects of the asset lifecycle as applicable to the asset: • 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;	**SOC2 - 1.** Azure assets are classified in accordance with Microsoft Online Services Classification Guidelines. The classification is documented, reviewed, and approved by the authorizing official. **C5 - 9.** Microsoft Azure has established policies for mobile computing devices to meet appropriate security practices prior to being connected to the production environment.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
• Remote deactivation, deletion or blocking; • Physical delivery and transport; • Dealing with incidents and vulnerabilities; and • Complete and irrevocable deletion of the data upon decommissioning.		
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.	**CM - 6.** Procedures to manage changes to network devices in the scope boundary have been established. **CM - 7.** Secure network configurations are applied and reviewed through defined change management procedures. **CM - 8.** The Technical Security Services team develops security configuration standards for systems in the physical environment that are consistent with industry-accepted hardening standards. These configurations are documented in system baselines, are reviewed annually, and relevant configuration changes are communicated to impacted teams. **CM - 9.** Datacenter change requests are classified, documented, and approved by the Operations Management Team.	No exceptions noted.
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. The decommissioning includes the complete and permanent deletion of the data or proper destruction of the media.	**SOC2 - 3.** Datacenter team controls the delivery and removal of information system components through tickets on the Global Datacenter Operations (GDCO) ticketing system. Delivery and removal of information system components is authorized by system owners. System components / assets are tracked in the GDCO ticketing database. **DS - 10.** Guidelines for the disposal of storage media have been established. **CM - 6.** Procedures to manage changes to network devices in the scope boundary have been established. **CM - 7.** Secure network configurations are applied and reviewed through defined change management procedures.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
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. Any assets handed over are provably returned upon termination of employment.	**SOC2 - 13.** Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees are provided Microsoft's Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage. Employees are required to acknowledge agreements to return Microsoft assets upon termination. **C5 - 9.** Microsoft Azure has established policies for mobile computing devices to meet appropriate security practices prior to being connected to the production environment.	No exceptions noted.
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. 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.	**SOC2 - 1.** Azure assets are classified in accordance with Microsoft Online Services Classification Guidelines. The classification is documented, reviewed, and approved by the authorizing official. **C5 - 9.** Microsoft Azure has established policies for mobile computing devices to meet appropriate security practices prior to being connected to the production environment.	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 Activity	Test Result
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. 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: • Faults in planning; • Unauthorised access; • Insufficient surveillance; • Insufficient air-conditioning; • Fire and smoke; • Water; • Power failure; and • Air ventilation and filtration. If the Cloud Service Provider uses premises or buildings operated by third parties to	**PE - 1.** Procedures to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors, have been established. **PE - 2.** Security verification and check-in for personnel requiring temporary access to the interior of the datacenter facility, including tour groups or visitors, are required. **PE - 4.** Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals. **PE - 6.** Datacenter Management team maintains and tests datacenter-managed environmental equipment within the facility according to documented policy and maintenance procedures. **PE - 7.** Environmental controls have been implemented to protect systems inside datacenter facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.	**Exception noted:** **PE - 4:** For 1 of 17 sampled datacenters, while there are various layers of physical access mechanisms that were determined to be properly implemented, two instances of physical access mechanisms were not properly administered: - A trash door that provides access to the loading area was not fully closed. - While keycards were required to enter the generator area, several generator enclosures within the area that are normally secured with temporary-use physical keys had broken or unsecured locks.

C5 Criteria	Azure Activity	Test Result
provide the Cloud Service, the document describes which security requirements the Cloud Service Provider places on these third parties. 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).		
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).	**BC - 4.** The BCP team conducts testing of the business continuity and disaster recovery plans established for Azure services, per the defined testing schedule for different loss scenario. Each loss scenario is tested at least annually. Issues identified during testing are resolved and plans are updated accordingly. **BC - 7.** A Datacenter Business Continuity Management (BCM) program to respond to Microsoft's Enterprise Business Continuance Initiative has been implemented and includes documented procedures for mapping processes to pre-defined enterprise functions, establishing recovery strategies as well as developing and conducting test scenarios that enable the BCM program to mitigate risks and vulnerabilities and respond to major disruptive events. **BC - 8.** A Datacenter Business Continuity Management Program defines business continuity planning and testing requirements for functions within the datacenters. Datacenters exercise, test and maintain the Datacenter Business Continuity Plan for the continued operations of critical processes and required resources in the event of a disruption at least annually. The 'Business Continuity Management Exercise and Test Program Framework' document establishes the basis and process for exercising and testing of the plans for continuity and resumption of critical datacenter processes. **DS - 6.** Critical Azure components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services. **DS - 7.** Customer data is automatically replicated within Azure to minimize isolated faults.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
	Customers are able to determine geographical regions of the data processing and storage, including data backups. **DS - 14.** Azure services are configured to automatically restore customer services upon detection of hardware and system failures.	
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). The security measures are designed to detect and prevent unauthorised access so that the information security of the cloud service is not compromised. The outer doors, windows and other construction elements exhibit an appropriate security level and withstand a burglary attempt for at least 10 minutes. The surrounding wall constructions as well as the locking mechanisms meet the associated requirements.	**PE - 1.** Procedures to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors, have been established. **PE - 2.** Security verification and check-in for personnel requiring temporary access to the interior of the datacenter facility, including tour groups or visitors, are required. **PE - 4.** Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.	**Exception noted:** **PE - 4:** For 1 of 17 sampled datacenters, while there are various layers of physical access mechanisms that were determined to be properly implemented, two instances of physical access mechanisms were not properly administered: - A trash door that provides access to the loading area was not fully closed. - While keycards were required to enter the generator area, several generator enclosures within the area that are normally secured with temporary-use physical keys had broken or unsecured locks.

C5 Criteria	Azure Activity	Test Result
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. Access controls are supported by an access control system. 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: • Specified procedure for the granting and revoking of access authorisations (cf. IDM-02) based on the principle of least authorisation ("least-privilege-principle") and as necessary for the performance of tasks ("need-to-know-principle"); • 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	**PE - 1.** Procedures to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors, have been established. **PE - 2.** Security verification and check-in for personnel requiring temporary access to the interior of the datacenter facility, including tour groups or visitors, are required. **PE - 3.** Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team. **PE - 4.** Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals. **PE - 5.** The datacenter facility is monitored 24x7 by security personnel. **Note:** Revocations of physical access authorizations for unused access are not automatically revoked within 2 months, or withdrawn within 6 months, as specified by C5 criteria PS-04. However, physical access to the datacenters is subject to quarterly user access reviews where access not needed to perform job responsibilities would be removed. Temporary access is also provisioned for a finite period of time before being expired and removed. Thus, ascertained that user access reviews and scheduled expiration / removal of temporary access addresses the risk and are appropriate to meet the C5 objective 5.5.	**Exception noted:** **PE - 4:** For 1 of 17 sampled datacenters, while there are various layers of physical access mechanisms that were determined to be properly implemented, two instances of physical access mechanisms were not properly administered: - A trash door that provides access to the loading area was not fully closed. - While keycards were required to enter the generator area, several generator enclosures within the area that are normally secured with temporary-use physical keys had broken or unsecured locks. **PE - 5:** For 1 of the 32 sampled cameras, the tapes were not retained in accordance

C5 Criteria	Azure Activity	Test Result
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.		with the documented operating procedures.
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: a) Structural Measures: Establishment of fire sections with a fire resistance duration of at least 90 minutes for all structural parts b) Technical Measures: • 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	**PE - 1.** Procedures to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors, have been established. **PE - 6.** Datacenter Management team maintains and tests datacenter-managed environmental equipment within the facility according to documented policy and maintenance procedures. **PE - 7.** Environmental controls have been implemented to protect systems inside datacenter facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
• Fire alarm system with reporting to the local fire department. c) Organisational Measures: • Regular fire protection inspections to check compliance with fire protection requirements; and • Regular fire protection exercises.		
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: a) Operational redundancy (N+1) in power and cooling supply 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). c) Maintenance (servicing, inspection, repair) of the utilities in accordance with the manufacturer's recommendations.	**PE - 6.** Datacenter Management team maintains and tests datacenter-managed environmental equipment within the facility according to documented policy and maintenance procedures. **PE - 7.** Environmental controls have been implemented to protect systems inside datacenter facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
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: • 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.		
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.	**PE - 5.** The datacenter facility is monitored 24x7 by security personnel. **PE - 7.** Environmental controls have been implemented to protect systems inside datacenter facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.	**Exception noted:** **PE - 5:** For 1 of the 32 sampled cameras, the tapes were not retained in accordance with the documented operating procedures.

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 Activity	Test Result
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. 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.	**BC - 10.** The network is monitored to ensure availability and address capacity issues in a timely manner. **C5 - 13.** Microsoft Capacity Management team projects future capacity requirements based on internal operational reports, revenue forecasts and inputs from internal component teams.	No exceptions noted.
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.	**BC - 10.** The network is monitored to ensure availability and address capacity issues in a timely manner. **SOC2 - 9.** Azure maintains and notifies customers of potential changes and events that may impact security or availability of the services through an online Service Dashboard. Changes to the security commitments and security obligations of Azure customers are updated on the Azure website in a timely manner. **LA - 1.** External access to Azure services and the customer data stored in the service requires authentication and is restricted based on customer configured authorization settings.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
	LA - 9. Service initializes the resource groups within the management portal based on the customer configured templates. Service allows customers to monitor and control the distribution of system resources created within the resource group in order to prevent resources from being congested. **VM - 12.** The availability of Azure services is monitored through third-party and internal tools, and the status is communicated through a Service Dashboard. **PI - 2.** Microsoft Azure management reviews portal performance monthly to evaluate compliance with customer SLA requirements.	
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.	**LA - 9.** Service initializes the resource groups within the management portal based on the customer configured templates. Service allows customers to monitor and control the distribution of system resources created within the resource group in order to prevent resources from being congested.	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: • 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.** A security policy that defines the information security rules and requirements for the Service environment has been established and communicated.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
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 malware detection and removal, these protection programs are updated at least daily.	**VM - 3.** A monitoring system to monitor the Azure platform for potential malicious activity and intrusion past service trust boundaries has been implemented.	No exceptions noted.
OPS-06 Policies and instructions for data backup and recovery are documented, communicated and provided in accordance with SP-01 regarding the following aspects. • 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).	**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. **DS - 5.** Backups of key Azure service components and secrets are performed regularly and stored in fault-tolerant (isolated) facilities. Backups are monitored and backup errors are investigated and followed-up on appropriately. **DS - 6.** Critical Azure components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services. **DS - 7.** Customer data is automatically replicated within Azure to minimize isolated faults. Customers are able to determine geographical regions of the data processing and storage, including data backups. **DS - 8.** Data Protection Services (DPS) backs up data for properties based on a defined schedule and upon request of the properties. Data is retained according to the data type identified by the property. DPS investigates backup errors and skipped files and follows up appropriately. **DS - 9.** Backup restoration procedures are defined and backup data integrity checks are performed through standard restoration activities. **DS - 13.** Production data on backup media is encrypted.	**Exception noted:** **DS - 8:** Management identified a vulnerability in the supporting third-party software used in scheduling of their internal offline backups. As a result, management paused backups, resulting in the control not operating effectively from February 22, 2025. **DS - 9:** Management identified a vulnerability in the supporting third-party software used in scheduling of their internal offline backups. As a result, management

C5 Criteria	Azure Activity	Test Result
	DS - 14. Azure services are configured to automatically restore customer services upon detection of hardware and system failures. **DS - 15.** Customer data is retained and removed per the defined terms within the Product Terms, when a customer's subscription expires, or is terminated. **OA - 1.** Administrative access to the Service environment is controlled through defined interfaces that require authentication using appropriate credentials. Privileges (i.e., read, write) are restricted to authorized personnel through designated channels based on job responsibilities.	paused backups, resulting in the control not operating effectively from February 22, 2025.
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.	**DS - 5.** Backups of key Azure service components and secrets are performed regularly and stored in fault-tolerant (isolated) facilities. Backups are monitored and backup errors are investigated and followed-up on appropriately. **DS - 8.** Data Protection Services (DPS) backs up data for properties based on a defined schedule and upon request of the properties. Data is retained according to the data type identified by the property. DPS investigates backup errors and skipped files and follows up appropriately.	**Exception noted:** **DS - 8:** Management identified a vulnerability in the supporting third-party software used in scheduling of their internal offline backups. As a result, management paused backups, resulting in the control not operating effectively from February 22, 2025.
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).	**DS - 5.** Backups of key Azure service components and secrets are performed regularly and stored in fault-tolerant (isolated) facilities. Backups are monitored and backup errors are investigated and followed-up on appropriately. **DS - 9.** Backup restoration procedures are defined and backup data integrity checks are performed through standard restoration activities. **BC - 1.** Business Continuity Plans (BCP) for critical Azure services, which provide roles and responsibilities and detailed procedures for recovery and reconstitution of systems to a known state per defined Recovery Time Objectives (RTOs) and	**Exception noted:** **DS - 9:** Management identified a vulnerability in the supporting third-party software used in scheduling of their internal offline backups.

C5 Criteria	Azure Activity	Test Result
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.	Recovery Point Objectives (RPOs), have been documented and published. Plans are reviewed on an annual basis, at a minimum. **BC - 4.** The BCP team conducts testing of the business continuity and disaster recovery plans established for Azure services, per the defined testing schedule for different loss scenario. Each loss scenario is tested at least annually. Issues identified during testing are resolved and plans are updated accordingly. **BC - 7.** A Datacenter Business Continuity Management (BCM) program to respond to Microsoft's Enterprise Business Continuance Initiative has been implemented and includes documented procedures for mapping processes to pre-defined enterprise functions, establishing recovery strategies as well as developing and conducting test scenarios that enable the BCM program to mitigate risks and vulnerabilities and respond to major disruptive events.	As a result, management paused backups, resulting in the control not operating effectively from February 22, 2025.
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.	**DS - 2.** Customer data communicated through Azure service interfaces is encrypted during transmission over external networks. Location-aware technologies are implemented within the Azure portal to identify and validate authentication sessions. **DS - 3.** Internal communication between key Azure components where customer data is transmitted / involved is secured using encryption. **DS - 5.** Backups of key Azure service components and secrets are performed regularly and stored in fault-tolerant (isolated) facilities. Backups are monitored and backup errors are investigated and followed-up on appropriately. **DS - 6.** Critical Azure components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services. **DS - 7.** Customer data is automatically replicated within Azure to minimize isolated faults. Customers are able to determine geographical regions of the data processing and storage, including data backups. **DS - 13.** Production data on backup media is encrypted.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
	PE - 1. Procedures to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors, have been established. **PE - 2.** Security verification and check-in for personnel requiring temporary access to the interior of the datacenter facility, including tour groups or visitors, are required.	
OPS-10 The Cloud Service Provider has established policies and instructions that govern the logging and monitoring of events 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: • 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.	**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. **C5 - 7.** 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. **C5 - 8.** Azure has established an Audit Log Management policy. Log and monitor access is restricted to only authorized staff with a business need to access such systems. **C5 - 10.** Microsoft Azure components are configured to use Coordinated Universal Time (UTC) time and the clocks are synchronized with the domain controller server. **VM - 1.** Azure platform components are configured to log and collect security events. **VM - 2.** Administrator activity in the Azure platform is logged. **VM - 4.** Procedures to investigate and respond to malicious events detected by the Azure monitoring system in a timely manner have been established. **VM - 9.** Network devices in the scope boundary are configured to log and collect security events, and monitored for compliance with established security standards. **VM - 12.** The availability of Azure services is monitored through third-party and internal tools, and the status is communicated through a Service Dashboard.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
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: • 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; • 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.	**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. **C5 - 5.** Customer metadata is collected, retained, and removed based on the documented procedures.	No exceptions noted.
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: • Access only for authorised users and systems; • Retention for the specified period; and	**C5 - 5.** Customer metadata is collected, retained, and removed based on the documented procedures. **C5 - 7.** 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. **C5 - 8.** Azure has established an Audit Log Management policy. Log and monitor access is restricted to only authorized staff with a business need to access such systems.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
• Deletion when further retention is no longer necessary for the purpose of collection.	**VM - 1.** Azure platform components are configured to log and collect security events. **VM - 2.** Administrator activity in the Azure platform is logged. **VM - 4.** Procedures to investigate and respond to malicious events detected by the Azure monitoring system in a timely manner have been established. **VM - 9.** Network devices in the scope boundary are configured to log and collect security events, and monitored for compliance with established security standards. **VM - 12.** The availability of Azure services is monitored through third-party and internal tools, and the status is communicated through a Service Dashboard.	
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). Identified events are automatically reported to the appropriate departments for prompt evaluation and action.	**VM - 1.** Azure platform components are configured to log and collect security events. **VM - 2.** Administrator activity in the Azure platform is logged. **VM - 3.** A monitoring system to monitor the Azure platform for potential malicious activity and intrusion past service trust boundaries has been implemented. **VM - 4.** Procedures to investigate and respond to malicious events detected by the Azure monitoring system in a timely manner have been established. **IM - 3.** The Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures. **IM - 4.** Incident post-mortem activities for severe incidents impacting the Azure environment are conducted.	No exceptions noted.
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	**C5 - 6.** 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.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
the data is possible. Log data is deleted if it is no longer required for the purpose for which they were collected. 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).	**C5 - 8.** Azure has established an Audit Log Management policy. Log and monitor access is restricted to only authorized staff with a business need to access such systems. **DS - 3.** Internal communication between key Azure components where customer data is transmitted / involved is secured using encryption.	
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. Interfaces are available to conduct forensic analyses and perform backups of infrastructure components and their network communication.	**C5 - 14.** Microsoft Azure has established forensic procedures to support potential legal action after an information security incident. **VM - 2.** Administrator activity in the Azure platform is logged.	No exceptions noted.
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).	**C5 - 6.** 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. **C5 - 8.** Azure has established an Audit Log Management policy. Log and monitor access is restricted to only authorized staff with a business need to access such systems. **CM - 3.** Key stakeholders approve prior to deploying a release into production based on documented change management procedures. **CM - 4.** Software releases and configuration changes to the Azure platform are tested based on established criteria prior to production implementation.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
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.	**C5 - 7.** 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.	No exceptions noted.
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: • Regular identification of vulnerabilities; • 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.	**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. **VM - 5.** Procedures to evaluate and implement Microsoft-released patches to Service components have been established. **VM - 6.** Procedures to monitor the Azure platform components for known security vulnerabilities have been established. Identified security vulnerabilities are remediated. **VM - 13.** Vulnerabilities for network devices are evaluated and mitigated based on documented procedures.	**Exception noted:** **VM - 6:** Internal Audit of Microsoft identified multiple vulnerabilities associated with five in-scope services that were not remediated in a timely manner within the expected SLA. No additional exceptions were noted in our independent testing.

C5 Criteria	Azure Activity	Test Result
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. The Cloud Service Provider assess the severity of the findings made in penetration tests according to defined criteria. 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.	**VM - 8.** Penetration testing of critical infrastructure components is performed at least annually based on documented Penetration testing procedures and findings are documented, tracked, and remediated.	No exceptions noted.
OPS-20 The Cloud Service Provider regularly measures, analyses and assesses the procedures with which vulnerabilities and incidents are handled to verify their continued suitability, appropriateness and effectiveness. Results are evaluated at least quarterly by accountable departments at the Cloud Service Provider to initiate continuous improvement actions and to verify their effectiveness.	**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. **IM - 1.** An incident management framework with defined processes, roles, and responsibilities for the detection, escalation and response of incidents, has been established and communicated. **IM - 6.** The Cyber Defense Operations Center (CDOC) team performs annual tests on the security incident response procedures.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
	SOC2 - 26. Microsoft Azure 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. **Note:** Azure 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.	
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. 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.	**IM - 1.** An incident management framework with defined processes, roles, and responsibilities for the detection, escalation and response of incidents, has been established and communicated. **SOC2 - 6.** Azure maintains a Customer Support website that describes the process for customers and other external users to inform about potential security issues and submit complaints. Reported issues are reviewed and addressed per documented incident management procedures. **SOC2 - 9.** Azure maintains and notifies customers of potential changes and events that may impact security or availability of the services through an online Service Dashboard. Changes to the security commitments and security obligations of Azure customers are updated on the Azure website in a timely manner.	No exceptions noted.
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	**VM - 5.** Procedures to evaluate and implement Microsoft-released patches to Service components have been established. **VM - 6.** Procedures to monitor the Azure platform components for known security vulnerabilities have been established. Identified security vulnerabilities are remediated. **VM - 13.** Vulnerabilities for network devices are evaluated and mitigated based on documented procedures.	**Exception noted:** **VM - 6:** Internal Audit of Microsoft identified multiple vulnerabilities associated with five in-scope services that were not remediated

C5 Criteria	Azure Activity	Test Result
and measures for timely remediation or mitigation are initiated within defined time windows.	**Note:** Azure 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.	in a timely manner within the expected SLA. No additional exceptions were noted in our independent testing.
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. 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.	**SOC2 - 15.** Azure has established baselines for OS deployments. Azure employs mechanisms to re-image production servers with the latest baseline configurations at least once a month or detect and troubleshoot exceptions or deviations from the baseline configuration in the production environment. The Azure OS and component teams review and update configuration settings and baseline configurations at least annually.	No exceptions noted.
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 on OIS-07 risk analysis to ensure the confidentiality and integrity of this data.	**OA - 18.** Azure network is segregated to separate customer traffic from management traffic. **SOC2 - 26.** Microsoft Azure 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. **LA - 3.** Logical segregation to restrict unauthorized access to other customer tenants is implemented.	No exceptions noted.

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 Activity	Test Result
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: • 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"); • 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;	**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. **OA - 1.** Administrative access to the Service environment is controlled through defined interfaces that require authentication using appropriate credentials. Privileges (i.e., read, write) are restricted to authorized personnel through designated channels based on job responsibilities. **OA - 2.** Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning employee, contractor, and service provider access to specific applications or information resources. **OA - 4.** User credentials adhere to established corporate standards and group policies for password requirements: - expiration - length - complexity - history Initial passwords have secure mechanisms in place for distribution and first-time use. For production domains where passwords are not in use, multi-factor authentication is 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.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
• 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.	**OA - 6.** Production domain-level user accounts are disabled after 90 days of inactivity. **OA - 10.** Users are granted access to network devices in the scope boundary upon receiving appropriate approvals. **OA - 21.** Access to production resources requires the use of a Secure Admin Workstation (SAW) which requires MFA for access **LA - 1.** External access to Azure services and the customer data stored in the service requires authentication and is restricted based on customer configured authorization settings.	
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.	**OA - 1.** Administrative access to the Service environment is controlled through defined interfaces that require authentication using appropriate credentials. Privileges (i.e., read, write) are restricted to authorized personnel through designated channels based on job responsibilities. **OA - 2.** Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning employee, contractor, and service provider access to specific applications or information resources. **OA - 3.** Procedures are in place to disable accounts on a timely basis, upon the user's termination. **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. **OA - 6.** Production domain-level user accounts are disabled after 90 days of inactivity. **OA - 7.** Procedures for granting Azure personnel temporary access to customer data and applications, upon appropriate approval for customer support or incident handling purposes, have been established.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
	OA - 10. Users are granted access to network devices in the scope boundary upon receiving appropriate approvals. **SOC2 - 25.** Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within the Azure environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Corporate, External, and Legal Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements. **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.	
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 components are required to unlock these accounts. 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.	**OA - 6.** Production domain-level user accounts are disabled after 90 days of inactivity.	No exceptions noted.
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	**OA - 3.** Procedures are in place to disable accounts on a timely basis, upon the user's termination.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
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.	**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. **OA - 6.** Production domain-level user accounts are disabled after 90 days of inactivity. **OA - 7.** Procedures for granting Azure personnel temporary access to customer data and applications, upon appropriate approval for customer support or incident handling purposes, have been established.	
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.	**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. **Note:** 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. Based on the access reviews, access modifications or withdrawals, if any, are performed as needed. Azure 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.	No exceptions noted.
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	**OA - 1.** Administrative access to the Service environment is controlled through defined interfaces that require authentication using appropriate credentials. Privileges (i.e., read, write) are restricted to authorized personnel through designated channels based on job responsibilities.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
access rights (cf. IDM-01) or a separate specific policy. 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. 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.	**OA - 2.** Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning employee, contractor, and service provider access to specific applications or information resources. **OA - 8.** Authentication over an encrypted Remote Desktop Connection is used for administrator access to the production environment. **OA - 20.** Alerts are generated when a break-glass account is used to access a production subscription. **SOC2 - 11.** Microsoft has defined disciplinary actions for employees and contingent staff that commit a security breach or violate Microsoft Security Policy. **VM - 2.** Administrator activity in the Azure platform is logged. **VM - 4.** Procedures to investigate and respond to malicious events detected by the Azure monitoring system in a timely manner have been established.	
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	**OA - 7.** Procedures for granting Azure personnel temporary access to customer data and applications, upon appropriate approval for customer support or incident handling purposes, have been established. **Note:** Azure 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.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
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.		
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: • 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.	**DS - 1.** Cryptographic certificates, keys, and customer access keys used for communication between Azure services and other internal components are stored securely and are rotated on a periodic basis. **DS - 4.** Cryptographic controls are used for information protection within the Azure platform based on the Azure Cryptographic Policy and Key Management procedures. The policies and procedures include the key rotation, archival and deactivation processes. Keys must have identifiable owners (binding keys to identities) and key management policies. **OA - 1.** Administrative access to the Service environment is controlled through defined interfaces that require authentication using appropriate credentials. Privileges (i.e., read, write) are restricted to authorized personnel through designated channels based on job responsibilities. **OA - 4.** User credentials adhere to established corporate standards and group policies for password requirements: - expiration - length - complexity - history	**Exception noted:** **DS - 1:** Three of 24 sampled secrets tested during the period 4/1/2024 to 12/31/2024 were not rotated as per the secret rotation cadence defined in the documented procedures. Further, tested 11 sampled secrets subsequent to December 31, 2024, and no additional exceptions were noted. Additionally, certain internal Microsoft platform keys were not rotated according to the prescribed cadence outlined in the internal policy. As mitigation, these keys were

C5 Criteria	Azure Activity	Test Result
• The server-side storage takes place using cryptographically strong hash functions. Deviations are evaluated by means of a risk analysis and mitigating measures derived from this are implemented.	Initial passwords have secure mechanisms in place for distribution and first-time use. For production domains where passwords are not in use, multi-factor authentication is enforced. **LA - 2.** Customer credentials used to access Azure services meet the applicable password policy requirements. Temporary credentials assigned to users by the service expire within 14 days and users are forced to change these credentials when using them for the first time. **LA - 4.** Customer data that is designated as "confidential" is protected while in storage within Azure services. **LA - 11.** One Time Passwords (OTPs) used for self-service password reset are randomly generated. OTPs expire after a pre-defined time limit. OTPs sent to the customer administrator are required to be validated before a password change is allowed. SSPR does not display user identifiable information during the password reset. Microsoft Entra ID password policy requirements are enforced on the new passwords supplied by customer administrators within SSPR portal. New passwords supplied by customer administrators are protected during transmission over external networks. **Note:** The initial password issued to internal users to access Azure production environment does not expire within 14 days, as specified by C5 criteria IDM-08. However, initial passwords, where applicable, follow the standard Microsoft password policy for age, length, complexity and expiration. The initial passwords are system generated and users are informed to change the password at first login. Additionally, production access which does not require the use of passwords uses multi-factor authentication. Further, once granted access to the production domain, access to production assets is provisioned through security groups. Thus, we can conclude that the design is appropriate to meet the C5 objective 5.7.	protected through other security practices, including additional encryption. Separately, as part of its investigation into the actions of Midnight Blizzard, Microsoft identified passwords and secrets impacting certain in-scope Azure services that were accessed by the threat actors through code repositories or Microsoft corporate email. Furthermore, Internal Audit of Microsoft identified multiple secrets associated with four in-scope services that were not rotated during the past year.
IDM-09 System components in the Cloud Service Provider's area of responsibility that are used to provide the cloud service,	**OA - 1.** Administrative access to the Service environment is controlled through defined interfaces that require authentication using appropriate credentials.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
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.	Privileges (i.e., read, write) are restricted to authorized personnel through designated channels based on job responsibilities. **OA - 4.** User credentials adhere to established corporate standards and group policies for password requirements: - expiration - length - complexity - history Initial passwords have secure mechanisms in place for distribution and first-time use. For production domains where passwords are not in use, multi-factor authentication is enforced. **OA - 8.** Authentication over an encrypted Remote Desktop Connection is used for administrator access to the production environment. **OA - 14.** Access to network devices in the scope boundary requires two-factor authentication and / or other secure mechanisms. **LA - 2.** Customer credentials used to access Azure services meet the applicable password policy requirements. Temporary credentials assigned to users by the service expire within 14 days and users are forced to change these credentials when using them for the first time. **LA - 11.** One Time Passwords (OTPs) used for self-service password reset are randomly generated. OTPs expire after a pre-defined time limit. OTPs sent to the customer administrator are required to be validated before a password change is allowed. SSPR does not display user identifiable information during the password reset. Microsoft Entra ID password policy requirements are enforced on the new passwords supplied by customer administrators within SSPR portal. New passwords supplied by customer administrators are protected during transmission over external networks. **C5 - 1.** Standard Operating Procedures (SOPs), that define the procedures required to operate and maintain the Service environment, have been	

C5 Criteria	Azure Activity	Test Result
	established and communicated to employees. SOPs are reviewed and approved annually by appropriate management.	

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 Activity	Test Result
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: • 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 are aligned with the 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.	**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. **DS - 4.** Cryptographic controls are used for information protection within the Azure platform based on the Azure Cryptographic Policy and Key Management procedures. The policies and procedures include the key rotation, archival and deactivation processes. Keys must have identifiable owners (binding keys to identities) and key management policies. **DS - 18.** Microsoft performs a risk assessment for encryption and key management to evaluate changes and updates to cryptography controls.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
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.	**DS - 2.** Customer data communicated through Azure service interfaces is encrypted during transmission over external networks. Location-aware technologies are implemented within the Azure portal to identify and validate authentication sessions. **DS - 4.** Cryptographic controls are used for information protection within the Azure platform based on the Azure Cryptographic Policy and Key Management procedures. The policies and procedures include the key rotation, archival and deactivation processes. Keys must have identifiable owners (binding keys to identities) and key management policies. **LA - 1.** External access to Azure services and the customer data stored in the service requires authentication and is restricted based on customer configured authorization settings. **OA - 17.** External traffic to the customer VM(s) is restricted to customer - enabled ports and protocols.	No exceptions noted.
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.	**DS - 1.** Cryptographic certificates, keys, and customer access keys used for communication between Azure services and other internal components are stored securely and are rotated on a periodic basis. **DS - 2.** Customer data communicated through Azure service interfaces is encrypted during transmission over external networks. Location-aware technologies are implemented within the Azure portal to identify and validate authentication sessions. **DS - 3.** Internal communication between key Azure components where customer data is transmitted / involved is secured using encryption. **DS - 4.** Cryptographic controls are used for information protection within the Azure platform based on the Azure Cryptographic Policy and Key Management procedures. The policies and procedures include the key rotation, archival and deactivation processes.	**Exception noted:** **DS - 1:** Three of 24 sampled secrets tested during the period 4/1/2024 to 12/31/2024 were not rotated as per the secret rotation cadence defined in the documented procedures. Further, tested 11 sampled secrets subsequent to December 31, 2024, and no additional exceptions were noted.

C5 Criteria	Azure Activity	Test Result
	Keys must have identifiable owners (binding keys to identities) and key management policies. **DS - 13.** Production data on backup media is encrypted. **DS - 17.** Azure provides customers the ability to manage their own data encryption keys. **LA - 4.** Customer data that is designated as "confidential" is protected while in storage within Azure services. **LA - 8.** The private root key belonging to the Azure services is protected from unauthorized access.	Additionally, certain internal Microsoft platform keys were not rotated according to the prescribed cadence outlined in the internal policy. As mitigation, these keys were protected through other security practices, including additional encryption. Separately, as part of its investigation into the actions of Midnight Blizzard, Microsoft identified passwords and secrets impacting certain in-scope Azure services that were accessed by the threat actors through code repositories or Microsoft corporate email. Furthermore, Internal Audit of Microsoft identified multiple secrets associated with four in-scope services that were not rotated during the past year.
CRY-04 Procedures and technical safeguards for secure key management in the area of	**C5 - 1.** Standard Operating Procedures (SOPs), that define the procedures required to operate and maintain the Service environment, have been	**Exception noted:** **DS - 1:**

C5 Criteria	Azure Activity	Test Result
responsibility of the Cloud Service Provider include at least the following aspects: • 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; • 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.	established and communicated to employees. SOPs are reviewed and approved annually by appropriate management. **DS - 1.** Cryptographic certificates, keys, and customer access keys used for communication between Azure services and other internal components are stored securely and are rotated on a periodic basis. **DS - 2.** Customer data communicated through Azure service interfaces is encrypted during transmission over external networks. Location-aware technologies are implemented within the Azure portal to identify and validate authentication sessions. **DS - 3.** Internal communication between key Azure components where customer data is transmitted / involved is secured using encryption. **DS - 4.** Cryptographic controls are used for information protection within the Azure platform based on the Azure Cryptographic Policy and Key Management procedures. The policies and procedures include the key rotation, archival and deactivation processes. Keys must have identifiable owners (binding keys to identities) and key management policies. **DS - 17.** Azure provides customers the ability to manage their own data encryption keys. **DS - 18.** Microsoft performs a risk assessment for encryption and key management to evaluate changes and updates to cryptography controls. **OA - 1.** Administrative access to the Service environment is controlled through defined interfaces that require authentication using appropriate credentials. Privileges (i.e., read, write) are restricted to authorized personnel through designated channels based on job responsibilities.	Three of 24 sampled secrets tested during the period 4/1/2024 to 12/31/2024 were not rotated as per the secret rotation cadence defined in the documented procedures. Further, tested 11 sampled secrets subsequent to December 31, 2024, and no additional exceptions were noted. Additionally, certain internal Microsoft platform keys were not rotated according to the prescribed cadence outlined in the internal policy. As mitigation, these keys were protected through other security practices, including additional encryption. Separately, as part of its investigation into the actions of Midnight Blizzard, Microsoft identified passwords and secrets impacting certain in-scope Azure services that were accessed by the threat actors through

C5 Criteria	Azure Activity	Test Result
		code repositories or Microsoft corporate email. Furthermore, Internal Audit of Microsoft identified multiple secrets associated with four in-scope services that were not rotated during the past year.

COS: Communication Security

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

C5 Criteria	Azure Activity	Test Result
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	**OA - 16.** Network filtering to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted service components is implemented. **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. **VM - 4.** Procedures to investigate and respond to malicious events detected by the Azure monitoring system in a timely manner have been established. **VM - 12.** The availability of Azure services is monitored through third-party and internal tools, and the status is communicated through a Service Dashboard. **IM - 2.** Events, thresholds, and metrics have been defined and configured to detect incidents and alert the associated Operations team.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
documented, communicated and provided in accordance with SP-01.		
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: • 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	**DS - 16.** Each Online Service's customer's data is segregated from other Online Services' customers' data, either logically or physically. **OA - 17.** External traffic to the customer VM(s) is restricted to customer - enabled ports and protocols. **OA - 18.** Azure network is segregated to separate customer traffic from management traffic. **LA - 3.** Logical segregation to restrict unauthorized access to other customer tenants is implemented.	No exceptions noted.
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	**VM - 6.** Procedures to monitor the Azure platform components for known security vulnerabilities have been established. Identified security vulnerabilities are remediated. **VM - 9.** Network devices in the scope boundary are configured to log and collect security events, and monitored for compliance with established security standards.	**Exception noted:** **VM - 6:** Internal Audit of Microsoft identified multiple vulnerabilities associated with five in-scope services that were not remediated

C5 Criteria	Azure Activity	Test Result
connection to trusted or untrusted networks according to the defined security requirements. 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. 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). 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.	**VM - 13.** Vulnerabilities for network devices are evaluated and mitigated based on documented procedures. **OA - 7.** Procedures for granting Azure personnel temporary access to customer data and applications, upon appropriate approval for customer support or incident handling purposes, have been established. **OA - 9.** User groups and Access Control Lists have been established to restrict access to network devices in the scope boundary. **OA - 10.** Users are granted access to network devices in the scope boundary upon receiving appropriate approvals. **OA - 13.** Access to network devices in the scope boundary is restricted through a limited number of entry points that require authentication over an encrypted connection. **OA - 14.** Access to network devices in the scope boundary requires two-factor authentication and / or other secure mechanisms. **OA - 18.** Azure network is segregated to separate customer traffic from management traffic. **SOC2 - 4.** 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. **SOC2 - 15.** Azure has established baselines for OS deployments. Azure employs mechanisms to re-image production servers with the latest baseline configurations at least once a month or detect and troubleshoot exceptions or deviations from the baseline configuration in the production environment. The Azure OS and component teams review and update configuration settings and baseline configurations at least annually. **SOC2 - 26.** Microsoft Azure 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.	in a timely manner within the expected SLA. No additional exceptions were noted in our independent testing.
COS-04 Each network perimeter is controlled by security gateways. The system access authorisation for cross-network	**OA - 16.** Network filtering to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted service components is implemented.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
access is based on a security assessment based on the requirements of the cloud customers.	**OA - 18.** Azure network is segregated to separate customer traffic from management traffic.	
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 create virtual machines are also physically or logically separated from other networks	**OA - 18.** Azure network is segregated to separate customer traffic from management traffic.	No exceptions noted.
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.	**DS - 3.** Internal communication between key Azure components where customer data is transmitted / involved is secured using encryption. **DS - 4.** Cryptographic controls are used for information protection within the Azure platform based on the Azure Cryptographic Policy and Key Management procedures. The policies and procedures include the key rotation, archival and deactivation processes. Keys must have identifiable owners (binding keys to identities) and key management policies. **DS - 16.** Each Online Service’s customer’s data is segregated from other Online Services’ customers’ data, either logically or physically. **LA - 3.** Logical segregation to restrict unauthorized access to other customer tenants is implemented. **OA - 18.** Azure network is segregated to separate customer traffic from management traffic.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
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.	**C5 - 3.** The architecture of the Azure production network is documented as part of the inventory process. Metadata describing the network attributes (i.e. location, tier, and connections) are dynamically generated and updated as part of standard operations.	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).	**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.	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 Activity	Test Result
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. 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. 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.	**C5 - 11.** Azure has published a standard set of APIs with an ecosystem of tools and libraries on the Azure Portal. **OA - 13.** Access to network devices in the scope boundary is restricted through a limited number of entry points that require authentication over an encrypted connection. **OA - 17.** External traffic to the customer VM(s) is restricted to customer - enabled ports and protocols. **OA - 19.** Microsoft Azure has published virtualization industry standards supported within its environment. **DS - 2.** Customer data communicated through Azure service interfaces is encrypted during transmission over external networks. Location-aware technologies are implemented within the Azure portal to identify and validate authentication sessions. **DS - 3.** Internal communication between key Azure components where customer data is transmitted / involved is secured using encryption.	No exceptions noted.
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: • Type, scope and format of the data the Cloud Service Provider provides to the cloud customer;	**OA - 19.** Microsoft Azure has published virtualization industry standards supported within its environment. **DS - 15.** Customer data is retained and removed per the defined terms within the Product Terms, when a customer’s subscription expires, or is terminated. **SOC2 - 28.** Customer data is accessible within agreed upon services in data formats compatible with providing those services. **C5 - 1.** Standard Operating Procedures (SOPs), that define the procedures required to operate and maintain the Service environment, have been	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
• 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. 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.	established and communicated to employees. SOPs are reviewed and approved annually by appropriate management.	
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). The deletion includes data in the cloud customer's environment, metadata and data stored in the data backups. The deletion procedures prevent recovery by forensic means.	**DS - 10.** Guidelines for the disposal of storage media have been established. **DS - 15.** Customer data is retained and removed per the defined terms within the Product Terms, when a customer’s subscription expires, or is terminated.	No exceptions noted.

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 Activity	Test Result
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. 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: • 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).	**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. **CM - 1.** Procedures for managing different types of changes, including emergency changes, to the Azure platform have been documented and communicated. **DS - 4.** Cryptographic controls are used for information protection within the Azure platform based on the Azure Cryptographic Policy and Key Management procedures. The policies and procedures include the key rotation, archival and deactivation processes. Keys must have identifiable owners (binding keys to identities) and key management policies. **SDL - 1.** Development of new features and changes to the Azure services follow a defined approach based on the Microsoft Security Development Lifecycle (SDL) methodology. The SDL review for each service is performed on an annual basis. **SDL - 2.** Applicable operational security and internal control requirements are documented, and implemented for Azure services based on Microsoft SDL methodology. **SDL - 4.** New features and major changes are developed and tested in separate environments prior to production implementation. Production data is not replicated in test or development environments. **SDL - 6.** Source code builds are scanned for malware prior to release to production. **SOC2 - 15.** Azure has established baselines for OS deployments. Azure employs mechanisms to re-image production servers with the latest baseline configurations at least once a month or detect and troubleshoot exceptions or deviations from the baseline configuration in the production environment. The Azure OS and component teams review and update configuration settings and baseline configurations at least annually.	**Exception noted:** **SDL - 1:** For 15 of the 36 sampled services, SDL review was not completed within the annual cadence. For the period 04/01/2024 to 08/31/2024, Internal Audit of Microsoft identified one additional sample that did not meet the annual SDL review cadence. Additionally, Internal Audit of Microsoft identified one sampled service in which two exceptions were not approved timely and by the appropriate personnel as per Microsoft's SDL Methodology.

C5 Criteria	Azure Activity	Test Result
DEV-02 In the case of outsourced development of the cloud service (or individual system components), specifications regarding the following aspects are contractually agreed between the Cloud Service Provider and the outsourced development contractor: • 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.	Not Applicable as Microsoft Azure does not outsource development work.	
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: • 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	**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. **CM - 1.** Procedures for managing different types of changes, including emergency changes, to the Azure platform have been documented and communicated. **CM - 2.** Secondary approval is required prior to all pull request check-ins to the production build, enforcing segregation among designated personal when implementing changes **CM - 6.** Procedures to manage changes to network devices in the scope boundary have been established.	**Exception noted:** **CM - 2:** Management self-identified a vulnerability that could have allowed a single individual to submit and approve code bypassing SOD controls at the pull request level by using two user accounts owned by the same individual (i.e. Corp and Alt accounts).

C5 Criteria	Azure Activity	Test Result
and releases for deployment in the production environment by authorised personnel or system components; • 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.	**CM - 9.** Datacenter change requests are classified, documented, and approved by the Operations Management Team.	Management identified and disclosed 31 related instances from a large quantity of pull requests where developers self-approved their pull requests before checking them into the production build, leveraging multiple user accounts that they owned. Additionally, tested 15 change samples subsequent to September 30, 2024 and no additional exceptions were noted.
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.	**IS - 4.** An information security education and awareness program that includes policy training and periodic security updates for Azure personnel has been established. **SDL - 1.** Development of new features and changes to the Azure services follow a defined approach based on the Microsoft Security Development Lifecycle (SDL) methodology. The SDL review for each service is performed on an annual basis. **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	**Exception noted:** **SDL - 1:** For 15 of the 36 sampled services, SDL review was not completed within the annual cadence. For the period 04/01/2024 to 08/31/2024, Internal Audit of Microsoft

C5 Criteria	Azure Activity	Test Result
	providers are trained to understand and comply with Microsoft's supplier code of conduct.	identified one additional sample that did not meet the annual SDL review cadence. Additionally, Internal Audit of Microsoft identified one sampled service in which two exceptions were not approved timely and by the appropriate personnel as per Microsoft's SDL Methodology.
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.	**CM - 1.** Procedures for managing different types of changes, including emergency changes, to the Azure platform have been documented and communicated. **CM - 3.** Key stakeholders approve prior to deploying a release into production based on documented change management procedures. **CM - 6.** Procedures to manage changes to network devices in the scope boundary have been established. **CM - 7.** Secure network configurations are applied and reviewed through defined change management procedures. **CM - 9.** Datacenter change requests are classified, documented, and approved by the Operations Management Team.	No exceptions noted.
DEV-06 Changes to the cloud service are subject to appropriate testing during software development and deployment. The type and scope of the tests correspond to the risk assessment. The tests are carried	**CM - 1.** Procedures for managing different types of changes, including emergency changes, to the Azure platform have been documented and communicated. **CM - 3.** Key stakeholders approve prior to deploying a release into production based on documented change management procedures.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
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. 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.	**CM - 4.** Software releases and configuration changes to the Azure platform are tested based on established criteria prior to production implementation. **CM - 5.** Implemented changes to the Azure platform 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. **CM - 7.** Secure network configurations are applied and reviewed through defined change management procedures. **CM - 9.** Datacenter change requests are classified, documented, and approved by the Operations Management Team. **CM - 10.** Secure configurations for datacenter software are applied through defined change management procedures including documentation, testing and approval.	
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 are logged and can therefore be traced back to the individuals or system components executing them.	**SDL - 5.** Azure Services use code repositories for managing source code changes. Procedures to approve code changes managed through source code repository are established. Code changes submitted to the repository are logged and can be traced to the individuals or system components executing them. **CM - 2.** Secondary approval is required prior to all pull request check-ins to the production build, enforcing segregation among designated personal when implementing changes. **CM - 3.** Key stakeholders approve prior to deploying a release into production based on documented change management procedures.	**Exception noted.** **CM - 2:** Management self-identified a vulnerability that could have allowed a single individual to submit and approve code bypassing SOD controls at the pull request level by using two user accounts owned by the same individual (i.e. Corp and Alt accounts). Management identified and disclosed 31 related instances from a large quantity of pull requests where developers self-approved their pull

C5 Criteria	Azure Activity	Test Result
		requests before checking them into the production build, leveraging multiple user accounts that they owned. Additionally, tested 15 change samples subsequent to September 30, 2024 and no additional exceptions were noted.
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 to the Azure platform 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, including emergency changes, to the Azure platform have been documented and communicated. **CM - 3.** Key stakeholders approve prior to deploying a release into production based on documented change management procedures. **CM - 5.** Implemented changes to the Azure platform 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. **CM - 6.** Procedures to manage changes to network devices in the scope boundary have been established. **CM - 7.** Secure network configurations are applied and reviewed through defined change management procedures.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
	CM - 9. Datacenter change requests are classified, documented, and approved by the Operations Management Team.	
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.** New features and major changes are developed and tested in separate environments prior to production implementation. Production data is not replicated in test or development environments. **SDL - 6.** 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 Activity	Test Result
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:	**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. **BC - 6.** Procedures for continuity of critical services provided by third-parties have been established. Contracts with third-parties are periodically monitored and reviewed for inconsistencies or non-conformance. Procedures to transition between critical third-parties based on results of monitoring are established.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
• 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; • 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.	**IS - 4.** An information security education and awareness program that includes policy training and periodic security updates for Azure personnel has been established. **SOC2 - 13.** Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees are provided Microsoft's Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage. Employees are required to acknowledge agreements to return Microsoft assets upon termination. **SOC2 - 14.** Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information, should be identified and regularly reviewed. **SOC2 - 25.** Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within the Azure environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Corporate, External, and Legal Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements. **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.	
SSO-02 Service providers and suppliers of the Cloud Service Provider undergo a risk assessment in accordance with the policies	**C5 - 1.** Standard Operating Procedures (SOPs), that define the procedures required to operate and maintain the Service environment, have been established	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
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. The risk assessment includes the identification, analysis, evaluation, handling and documentation of risks with regard to the following aspects: • 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; • 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.	and communicated to employees. SOPs are reviewed and approved annually by appropriate management. **C5 - 2.** 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. **SOC2 - 25.** Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within the Azure environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Corporate, External, and Legal Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements. **SOC2 - 26.** Microsoft Azure 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. **BC - 6.** Procedures for continuity of critical services provided by third-parties have been established. Contracts with third-parties are periodically monitored and reviewed for inconsistencies or non-conformance. Procedures to transition between critical third-parties based on results of monitoring are established.	
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: • Company name; • Address;	**SOC2 - 25.** Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within the Azure environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Corporate, External, and Legal Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements. **C5 - 2.** 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.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
• 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. The information in the list is checked at least annually for completeness, accuracy and validity.	**BC - 6.** Procedures for continuity of critical services provided by third-parties have been established. Contracts with third-parties are periodically monitored and reviewed for inconsistencies or non-conformance. Procedures to transition between critical third-parties based on results of monitoring are established.	
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. 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: • reports on the quality of the service provided; • certificates of the management systems' compliance with international standards;	**SOC2 - 4.** 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. **SOC2 - 20.** Azure performs periodic Information Security Management System (ISMS) reviews and reviews results 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. Audit activities are planned and agreed upon in advance by stakeholders and any access required to perform the audits requires approval. **SOC2 - 25.** Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within the Azure environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g.,	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
• 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. 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. Identified violations and deviations are subjected to analysis, evaluation and treatment in accordance with the risk management procedure (cf. OIS-07).	Corporate, External, and Legal Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements. **SOC2 - 26.** Microsoft Azure 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. **SOC2 - 27.** Microsoft Azure undergoes independent audits and assessments, to monitor and verify compliance with security requirements, at least annually. Findings are recorded, reviewed, prioritized, and remediation plans are developed. **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. **BC - 6.** Procedures for continuity of critical services provided by third-parties have been established. Contracts with third-parties are periodically monitored and reviewed for inconsistencies or non-conformance. Procedures to transition between critical third-parties based on results of monitoring are established.	
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). Exit strategies are aligned with operational continuity plans and include the following aspects: • Analysis of the potential costs, impacts, resources and timing of the transition of a	**BC - 6.** Procedures for continuity of critical services provided by third-parties have been established. Contracts with third-parties are periodically monitored and reviewed for inconsistencies or non-conformance. Procedures to transition between critical third-parties based on results of monitoring are established.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
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.		

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 Activity	Test Result
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. 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.	**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. **IM - 1.** An incident management framework with defined processes, roles, and responsibilities for the detection, escalation and response of incidents, has been established and communicated. **IM - 3.** The Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
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. Customers affected by security incidents are informed in a timely and appropriate manner.	**SOC2 - 9.** Azure maintains and notifies customers of potential changes and events that may impact security or availability of the services through an online Service Dashboard. Changes to the security commitments and security obligations of Azure customers are updated on the Azure website in a timely manner.	
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.	**IM - 2.** Events, thresholds, and metrics have been defined and configured to detect incidents and alert the associated Operations team. **IM - 3.** The Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures. **IM - 4.** Incident post-mortem activities for severe incidents impacting the Azure environment are conducted. **VM - 8.** Penetration testing of critical infrastructure components is performed at least annually based on documented Penetration testing procedures and findings are documented, tracked, and remediated. **PE - 8.** Datacenter physical security management reviews and approves the incident response procedures on a yearly basis. The incident security response procedures detail the appropriate steps to be taken in the event of a security incident and the methods to report security weaknesses.	No exceptions noted.
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.	**C5 - 14.** Microsoft Azure has established forensic procedures to support potential legal action after an information security incident. **SOC2 - 9.** Azure maintains and notifies customers of potential changes and events that may impact security or availability of the services through an online Service Dashboard. Changes to the security commitments and security obligations of Azure customers are updated on the Azure website in a timely manner.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
	IM - 4. Incident post-mortem activities for severe incidents impacting the Azure environment are conducted.	
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. 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.	**IS - 3.** Management has established defined roles and responsibilities to oversee implementation of the Security Policy across Azure. **IM - 1.** An incident management framework with defined processes, roles, and responsibilities for the detection, escalation and response of incidents, has been established and communicated. **SOC2 - 13.** Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees are provided Microsoft’s Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage. Employees are required to acknowledge agreements to return Microsoft assets upon termination. **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.	No exceptions noted.
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.	**IM - 1.** An incident management framework with defined processes, roles, and responsibilities for the detection, escalation and response of incidents, has been established and communicated. **IM - 2.** Events, thresholds, and metrics have been defined and configured to detect incidents and alert the associated Operations team. **IM - 3.** The Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures. **IM - 4.** Incident post-mortem activities for severe incidents impacting the Azure environment are conducted.	No exceptions noted.

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 Activity	Test Result
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. 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.	**BC - 3.** Azure has developed a Business Continuity and Disaster Recovery (BC / DR) Standard Operating Procedure and documentation that includes the defined information security and availability requirements. **BC - 7.** A Datacenter Business Continuity Management (BCM) program to respond to Microsoft's Enterprise Business Continuance Initiative has been implemented and includes documented procedures for mapping processes to pre-defined enterprise functions, establishing recovery strategies as well as developing and conducting test scenarios that enable the BCM program to mitigate risks and vulnerabilities and respond to major disruptive events.	No exceptions noted.
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: • Possible scenarios based on a risk analysis; • Identification of critical products and services	**BC - 1.** Business Continuity Plans (BCP) for critical Azure services, which provide roles and responsibilities and detailed procedures for recovery and reconstitution of systems to a known state per defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), have been documented and published. Plans are reviewed on an annual basis, at a minimum. **BC - 3.** Azure has developed a Business Continuity and Disaster Recovery (BC / DR) Standard Operating Procedure and documentation that includes the defined information security and availability requirements. **BC - 5.** Risk assessments are conducted to identify and assess business continuity risks related to Azure services.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
• 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.	**BC - 7.** A Datacenter Business Continuity Management (BCM) program to respond to Microsoft's Enterprise Business Continuance Initiative has been implemented and includes documented procedures for mapping processes to pre-defined enterprise functions, establishing recovery strategies as well as developing and conducting test scenarios that enable the BCM program to mitigate risks and vulnerabilities and respond to major disruptive events.	
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".	**BC - 1.** Business Continuity Plans (BCP) for critical Azure services, which provide roles and responsibilities and detailed procedures for recovery and reconstitution of systems to a known state per defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), have been documented and published. Plans are reviewed on an annual basis, at a minimum. **BC - 4.** The BCP team conducts testing of the business continuity and disaster recovery plans established for Azure services, per the defined testing schedule	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
Business continuity plans and contingency plans take the following aspects into account: • 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.	for different loss scenario. Each loss scenario is tested at least annually. Issues identified during testing are resolved and plans are updated accordingly. **BC - 8.** A Datacenter Business Continuity Management Program defines business continuity planning and testing requirements for functions within the datacenters. Datacenters exercise, test and maintain the Datacenter Business Continuity Plan for the continued operations of critical processes and required resources in the event of a disruption at least annually. The 'Business Continuity Management Exercise and Test Program Framework' document establishes the basis and process for exercising and testing of the plans for continuity and resumption of critical datacenter processes.	
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	**BC - 1.** Business Continuity Plans (BCP) for critical Azure services, which provide roles and responsibilities and detailed procedures for recovery and reconstitution of systems to a known state per defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), have been documented and published. Plans are reviewed on an annual basis, at a minimum. **BC - 4.** The BCP team conducts testing of the business continuity and disaster recovery plans established for Azure services, per the defined testing schedule	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
into account for future operational continuity measures.	for different loss scenario. Each loss scenario is tested at least annually. Issues identified during testing are resolved and plans are updated accordingly. **BC - 8.** A Datacenter Business Continuity Management Program defines business continuity planning and testing requirements for functions within the datacenters. Datacenters exercise, test and maintain the Datacenter Business Continuity Plan for the continued operations of critical processes and required resources in the event of a disruption at least annually. The 'Business Continuity Management Exercise and Test Program Framework' document establishes the basis and process for exercising and testing of the plans for continuity and resumption of critical datacenter processes.	

COM: Compliance

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

C5 Criteria	Azure 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.	**SOC2 - 18.** Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements for each information system and the organization, should be explicitly defined, documented, and kept up to date. **SOC2 - 19.** A compliance program is managed with representation from various cross-functional teams and external parties to identify and manage compliance with relevant statutory, regulatory and contractual requirements.	No exceptions noted.
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:	**SOC2 - 20.** Azure performs periodic Information Security Management System (ISMS) reviews and reviews results 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.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
• Restriction to read-only access to system components in accordance with the agreed audit plan and as necessary to perform the activities; • 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.	Audit activities are planned and agreed upon in advance by stakeholders and any access required to perform the audits requires approval. **SOC2 - 27.** Microsoft Azure undergoes independent audits and assessments, to monitor and verify compliance with security requirements, at least annually. Findings are recorded, reviewed, prioritized, and remediation plans are developed.	
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 . 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).	**SOC2 - 18.** Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements for each information system and the organization, should be explicitly defined, documented, and kept up to date. **SOC2 - 20.** Azure performs periodic Information Security Management System (ISMS) reviews and reviews results 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. Audit activities are planned and agreed upon in advance by stakeholders and any access required to perform the audits requires approval. **SOC2 - 26.** Microsoft Azure 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. **SOC2 - 27.** Microsoft Azure undergoes independent audits and assessments, to monitor and verify compliance with security requirements, at least annually. Findings are recorded, reviewed, prioritized, and remediation plans are developed.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
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.	**IS - 3.** Management has established defined roles and responsibilities to oversee implementation of the Security Policy across Azure. **PI - 2.** Microsoft Azure management reviews portal performance monthly to evaluate compliance with customer SLA requirements. **SOC2 - 20.** Azure performs periodic Information Security Management System (ISMS) reviews and reviews results 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. Audit activities are planned and agreed upon in advance by stakeholders and any access required to perform the audits requires approval. **SOC2 - 26.** Microsoft Azure 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.	No exceptions noted.

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 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 - 4.** 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 Activity	Test Result
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 - 4.** 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-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.	**C5 - 4.** 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-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. 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.	**C5 - 4.** 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.

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 Activity	Test Result
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. 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: • Instructions for secure configuration; • Information sources on known vulnerabilities and update mechanisms; • Error handling and logging mechanisms; • Authentication mechanisms;	**SOC2 - 7.** Azure 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. **SOC2 - 8.** Azure maintains and distributes an accurate system description to authorized users. **SOC2 - 10.** Prior to engaging in Azure services, customers are required to review and agree with the acceptable use of data and the Azure service, as well as security and privacy requirements, which are defined in the Product Terms, Microsoft Online Subscription Agreement, Azure service Privacy Statement and Technical Overview of the Security Features in Azure service. **C5 - 11.** Azure has published a standard set of APIs with an ecosystem of tools and libraries on the Azure Portal.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
• 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. The information is maintained so that it is applicable to the cloud service provided in the version intended for productive use.		
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. The procedures for identifying such vulnerabilities are part of the software development process and, depending on a risk assessment, include the following activities: • 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. The severity of identified vulnerabilities is assessed according to defined criteria and	**CM - 5.** Implemented changes to the Azure platform 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. **SDL - 1.** Development of new features and changes to the Azure services follow a defined approach based on the Microsoft Security Development Lifecycle (SDL) methodology. The SDL review for each service is performed on an annual basis. **SDL - 2.** Applicable operational security and internal control requirements are documented, and implemented for Azure services based on Microsoft SDL methodology. **SDL - 6.** Source code builds are scanned for malware prior to release to production. **VM - 5.** Procedures to evaluate and implement Microsoft-released patches to Service components have been established. **VM - 6.** Procedures to monitor the Azure platform components for known security vulnerabilities have been established. Identified security vulnerabilities are remediated. **VM - 8.** Penetration testing of critical infrastructure components is performed at least annually based on documented Penetration testing procedures and findings are documented, tracked, and remediated. **VM - 13.** Vulnerabilities for network devices are evaluated and mitigated based on documented procedures.	**Exceptions Noted:** **SDL - 1:** For 15 of the 36 sampled services, SDL review was not completed within the annual cadence. For the period 04/01/2024 to 08/31/2024, Internal Audit of Microsoft identified one additional sample that did not meet the annual SDL review cadence. Additionally, Internal Audit of Microsoft identified one sampled service in which two exceptions were not approved timely and by the appropriate personnel as per Microsoft's SDL Methodology. **VM - 6:**

C5 Criteria	Azure Activity	Test Result
measures are taken to immediately eliminate or mitigate them.	**SOC2 - 15.** Azure has established baselines for OS deployments. Azure employs mechanisms to re-image production servers with the latest baseline configurations at least once a month or detect and troubleshoot exceptions or deviations from the baseline configuration in the production environment. The Azure OS and component teams review and update configuration settings and baseline configurations at least annually.	Internal Audit of Microsoft identified multiple vulnerabilities associated with five in-scope services that were not remediated in a timely manner within the expected SLA. No additional exceptions were noted in our independent testing.
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. The presentation of the vulnerabilities follows the Common Vulnerability Scoring System (CVSS). 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. 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.	**VM - 5.** Procedures to evaluate and implement Microsoft-released patches to Service components have been established. **VM - 6.** Procedures to monitor the Azure platform components for known security vulnerabilities have been established. Identified security vulnerabilities are remediated. **VM - 11.** Microsoft operating system updates for virtual machines are made available through Microsoft Security Response Center (MSRC) site and Windows Update. **VM - 13.** Vulnerabilities for network devices are evaluated and mitigated based on documented procedures. **SOC2 - 15.** Azure has established baselines for OS deployments. Azure employs mechanisms to re-image production servers with the latest baseline configurations at least once a month or detect and troubleshoot exceptions or deviations from the baseline configuration in the production environment. The Azure OS and component teams review and update configuration settings and baseline configurations at least annually.	**Exception noted:** **VM - 6:** Internal Audit of Microsoft identified multiple vulnerabilities associated with five in-scope services that were not remediated in a timely manner within the expected SLA. No additional exceptions were noted in our independent testing.

C5 Criteria	Azure Activity	Test Result
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. The information is detailed enough to allow cloud users to check the following aspects, insofar as they are applicable to the cloud service: • 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. The logged information is protected from unauthorised access and modification and can be deleted by the Cloud Customer. If the cloud customer is responsible for the activation or type and scope of logging, the Cloud Service Provider must provide appropriate logging capabilities.	**VM - 1.** Azure platform components are configured to log and collect security events. **VM - 2.** Administrator activity in the Azure platform is logged. **VM - 3.** A monitoring system to monitor the Azure platform for potential malicious activity and intrusion past service trust boundaries has been implemented. **VM - 10.** Azure provides logging mechanisms that can be configured by customers to log activities and performance metrics. **LA - 1.** External access to Azure services and the customer data stored in the service requires authentication and is restricted based on customer configured authorization settings. **LA - 9.** Service initializes the resource groups within the management portal based on the customer configured templates. Service allows customers to monitor and control the distribution of system resources created within the resource group in order to prevent resources from being congested. **SOC2 - 9.** Azure maintains and notifies customers of potential changes and events that may impact security or availability of the services through an online Service Dashboard. Changes to the security commitments and security obligations of Azure customers are updated on the Azure website in a timely manner. **C5 - 5.** Customer metadata is collected, retained, and removed based on the documented procedures. **C5 - 6.** 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. **C5 - 7.** 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.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
	C5 - 8. Azure has established an Audit Log Management policy. Log and monitor access is restricted to only authorized staff with a business need to access such systems.	
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. These authentication mechanisms are set up at all access points that allow users, IT components or applications to interact with the cloud service. For privileged users, IT components or applications, these authentication mechanisms are enforced.	**LA - 1.** External access to Azure services and the customer data stored in the service requires authentication and is restricted based on customer configured authorization settings. **LA - 2.** Customer credentials used to access Azure services meet the applicable password policy requirements. Temporary credentials assigned to users by the service expire within 14 days and users are forced to change these credentials when using them for the first time. **LA - 11.** One Time Passwords (OTPs) used for self-service password reset are randomly generated. OTPs expire after a pre-defined time limit. OTPs sent to the customer administrator are required to be validated before a password change is allowed. SSPR does not display user identifiable information during the password reset. Microsoft Entra ID password policy requirements are enforced on the new passwords supplied by customer administrators within SSPR portal. New passwords supplied by customer administrators are protected during transmission over external networks. **OA - 4.** User credentials adhere to established corporate standards and group policies for password requirements: - expiration - length - complexity - history Initial passwords have secure mechanisms in place for distribution and first-time use. For production domains where passwords are not in use, multi-factor authentication is enforced. **OA - 14.** Access to network devices in the scope boundary requires two-factor authentication and / or other secure mechanisms.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
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 - 5.** User sessions within Azure can be configured by customers to 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: • 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. • The user is informed about changing or resetting the password. • The server-side storage takes place using state-of-the-art cryptographically strong	**LA - 2.** Customer credentials used to access Azure services meet the applicable password policy requirements. Temporary credentials assigned to users by the service expire within 14 days and users are forced to change these credentials when using them for the first time. **LA - 11.** One Time Passwords (OTPs) used for self-service password reset are randomly generated. OTPs expire after a pre-defined time limit. OTPs sent to the customer administrator are required to be validated before a password change is allowed. SSPR does not display user identifiable information during the password reset. Microsoft Entra ID password policy requirements are enforced on the new passwords supplied by customer administrators within SSPR portal. New passwords supplied by customer administrators are protected during transmission over external networks.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
hash functions in combination with at least 32-bit long salt values.		
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. 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").	**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. **OA - 1.** Administrative access to the Service environment is controlled through defined interfaces that require authentication using appropriate credentials. Privileges (i.e., read, write) are restricted to authorized personnel through designated channels based on job responsibilities. **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. **SDL - 3.** Responsibilities for submitting and approving production deployments are segregated within the Azure teams. **CM - 2.** Secondary approval is required prior to all pull request check-ins to the production build, enforcing segregation among designated personal when implementing changes.	**Exception noted:** **CM - 2:** Management self-identified a vulnerability that could have allowed a single individual to submit and approve code bypassing SOD controls at the pull request level by using two user accounts owned by the same individual (i.e. Corp and Alt accounts). Management identified and disclosed 31 related instances from a large quantity of pull requests where developers self-approved their pull requests before checking them into the production build, leveraging multiple user accounts that they owned. Additionally, tested 15 change samples subsequent to September 30, 2024 and no additional exceptions were noted.

C5 Criteria	Azure Activity	Test Result
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. 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 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).	**OA - 1.** Administrative access to the Service environment is controlled through defined interfaces that require authentication using appropriate credentials. Privileges (i.e., read, write) are restricted to authorized personnel through designated channels based on job responsibilities. **OA - 2.** Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning employee, contractor, and service provider access to specific applications or information resources. **OA - 7.** Procedures for granting Azure personnel temporary access to customer data and applications, upon appropriate approval for customer support or incident handling purposes, have been established. **CM - 1.** Procedures for managing different types of changes, including emergency changes, to the Azure platform have been documented and communicated. **CM - 3.** Key stakeholders approve prior to deploying a release into production based on documented change management procedures. **CM - 4.** Software releases and configuration changes to the Azure platform are tested based on established criteria prior to production implementation. **SDL - 4.** New features and major changes are developed and tested in separate environments prior to production implementation. Production data is not replicated in test or development environments. **VM - 5.** Procedures to evaluate and implement Microsoft-released patches to Service components have been established. **VM - 6.** Procedures to monitor the Azure platform components for known security vulnerabilities have been established. Identified security vulnerabilities are remediated.	**Exception noted:** **VM - 6:** Internal Audit of Microsoft identified multiple vulnerabilities associated with five in-scope services that were not remediated in a timely manner within the expected SLA. No additional exceptions were noted in our independent testing.
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.	**CM - 1.** Procedures for managing different types of changes, including emergency changes, to the Azure platform have been documented and communicated.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
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.	**CM - 4.** Software releases and configuration changes to the Azure platform are tested based on established criteria prior to production implementation. **CM - 5.** Implemented changes to the Azure platform 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. **CM - 6.** Procedures to manage changes to network devices in the scope boundary have been established. **CM - 7.** Secure network configurations are applied and reviewed through defined change management procedures.	
PSS-11 If cloud customers operate virtual machines or containers with the cloud service, the Cloud Service Provider must ensure the following aspects: • 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 the Cloud Customer, the Cloud Service Provider appropriately inform the Cloud Customer of the changes made to the previous version. • In addition, these images provided by the Cloud Service Provider are hardened according to generally accepted industry standards.	**SOC2 - 15.** Azure has established baselines for OS deployments. Azure employs mechanisms to re-image production servers with the latest baseline configurations at least once a month or detect and troubleshoot exceptions or deviations from the baseline configuration in the production environment. The Azure OS and component teams review and update configuration settings and baseline configurations at least annually. **LA - 12.** Images may be customized and access to images may be restricted by the customer. Updates to available images are communicated to through customer-facing websites. **OA - 19.** Microsoft Azure has published virtualization industry standards supported within its environment. **Note:** Hardened images available through the Azure Marketplace are published by third-party vendors. Microsoft expects customers to hardened / customize images as per customer requirements. Thus, we can conclude that the design is appropriate to meet the C5 objective 5.17.	No exceptions noted.

C5 Criteria	Azure Activity	Test Result
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. This must be ensured by the cloud architecture.	**DS - 7.** Customer data is automatically replicated within Azure to minimize isolated faults. Customers are able to determine geographical regions of the data processing and storage, including data backups.	No exceptions noted.

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

Control ID	Control Activity	Test Procedures	Results of Tests
IS - 1	A security policy that defines the information security rules and requirements for the Service environment has been established and communicated.	• Inquired of management if a documented security policy that specifies the documented rules and requirements applicable to the Microsoft Azure environment exists. • Obtained and inspected Microsoft Azure's Information Security Policy and ascertained that it addressed applicable information security requirements. • Observed that the Security Policy document was published and communicated to Microsoft Azure employees and the relevant third parties. • Inspected the Security Policy to determine if the security objectives were derived from the corporate objectives and business processes, relevant laws and regulations as well as the current and future expected threat environment with respect to information security.	No exceptions noted.
IS - 2	The Security Policy is reviewed and approved annually by appropriate management.	• Inquired of management to gain an understanding of the process for reviewing and approving the Microsoft Azure security policy. • Obtained and inspected the latest policy review performed for the Microsoft Azure security policy and approval provided by management.	No exceptions noted.
IS - 3	Management has established defined roles and responsibilities to oversee implementation of the Security Policy across Azure.	• Inquired of management to gain an understanding of the implementation of security policy requirements within Microsoft Azure through the designation of roles and responsibilities. • Inspected relevant documentation (e.g., SOPs) to test if roles and responsibilities for implementation of the security policy requirements were defined and documented.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
IS - 4	An information security education and awareness program that includes policy training and periodic security updates for Azure personnel has been established.	• Inquired of 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 security policy requirements, and was updated as needed. • Inspected the training material related to datacenter personnel and ascertained that it incorporated awareness on security risks and was updated as needed.	No exceptions noted.
OA - 1	Administrative access to the Service environment is controlled through defined interfaces that require authentication using appropriate credentials. Privileges (i.e., read, write) are restricted to authorized personnel through designated channels based on job responsibilities.	• Inquired of management to understand the procedures in place for accessing the Azure production environment, including data backups and datacenters. • For a sample of Azure services, obtained and inspected authentication mechanisms and associated security groups to ascertain that privileged access to the Azure Management Portal and other administrative tools required authentication and was restricted to authorized entities based on job responsibilities. • Obtained and inspected a list of users with privileged access and ascertained that user access to the relevant domains was restricted to defined security user groups and membership. • Obtained and inspected the current listing of user accounts, including their respective user IDs within the Azure domains, 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 employee, contractor, and service provider access to specific applications or information resources.	• Inquired of management if access requests require approval by the security group owner or asset owner using the account management tool. • For a sample of one user and security group, observed the enforcement of approval rule configuration to ascertain that access is created/obtained after the appropriate approvals.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		• For a sample of security groups / individual user access, obtained and inspected approvals prior to provisioning access to specific applications or information resources.	
OA - 3	Procedures are in place to disable accounts on a timely basis, upon the user's termination.	• Inquired of management if procedures for disabling terminated user accounts within a defined time period after the user's termination date are established. • Obtained and inspected the applicable configuration settings to ascertain that accounts are disabled on a timely basis upon the user's termination. • Selected a sample of terminated users and inspected Active Directory (AD) domain logs to ascertain that corporate accounts and AD production domain accounts were disabled by an automated job within five days of the user's termination date.	No exceptions noted.
OA - 4	User credentials adhere to established corporate standards and group policies for password requirements: - expiration - length - complexity - history Initial passwords have secure mechanisms in place for distribution and first-time use. For production domains where passwords are not in use, multi-factor authentication is enforced.	• Inquired of management to gain an understanding of the implementation of password standards (e.g., length, complexity, age) and acceptable use guidelines for user credentials created on production domains where passwords are in use. • Obtained and inspected the group policies enforced on the corporate domain and production domains where passwords are in use. • For production domains where passwords are not in use, observed use of multi-factor authentication with a security PIN and certificate. • Inquired of management if temporary passwords were required to be changed on first use and expire on a timely basis. • Obtained sample notifications for the production domains and observed the security mechanisms in place for password distribution and first-time use.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
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.	• Inquired of management to gain an understanding of the process for performing periodic user access reviews for Microsoft Azure. • 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	Production domain-level user accounts are disabled within 90 days of inactivity.	• Inquired of management if procedures for disabling user accounts that have been inactive for 90 days 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. • For a sampled user, obtained and inspected the last login date and account status to ascertain that the account was disabled timely after the inactivity period.	No exceptions noted.
OA - 7	Procedures for granting Azure personnel temporary access to customer data and applications, upon appropriate approval for customer support or incident handling purposes, have been established.	• 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. • Observed the customer data access approval process and ascertained that Azure personnel can only obtain access to customer data after appropriate approval from the customers.	No exceptions noted.
OA - 8	Authentication over an encrypted Remote Desktop Connection is used for administrator access to the production environment.	• Inquired of management to understand the authentication enforced during an RDP session to production environment and encryption of an RDP session.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		• Observed the authentication mechanisms and corresponding encrypted channel to ascertain that login attempt to remotely connect to the production environment was authenticated and over an encrypted connection.	
OA - 9	User groups and Access Control Lists have been established to restrict access to network devices in the scope boundary.	• Inquired of management if user groups are managed via the Active Directory, and Access Control Lists (ACLs) are established to restrict access to network devices. • Obtained and inspected configuration for a sample of network devices, and ascertained that TACACS+ was used for authentication and authorization of access, and that ACLs were applied.	No exceptions noted.
OA - 10	Users are granted access to network devices in the scope boundary upon receiving appropriate approvals.	• Inquired of management regarding the procedures in place to grant access to new users for network devices in the scope boundary. • Observed the approval process to ascertain that access to network devices was granted upon receiving appropriate approvals from the manager. • For a sample of access provisions, obtained and inspected the approvals and ascertained that access is provisioned after receiving appropriate approvals.	No exceptions noted.
OA - 13	Access to network devices in the scope boundary is restricted through a limited number of entry points that require authentication over an encrypted connection.	• Inquired of management if access to the network devices is restricted through a limited number of entry points which require authentication over an encrypted Remote Desktop connection. • Inspected the Network Account Management SOP and ascertained that procedures to restrict user access to network devices in the scope boundary, through a limited number of entry points that required authentication over an encrypted connection were established.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		• For a sampled jumpbox server, through observation, ascertained that remote access to network devices involved logging into a jumpbox server using domain credentials and a smart card followed by a log in to the internal-facing terminal server using domain credentials. Also, noted that Secure Shell (SSH) was enforced to access the network device. • Obtained and inspected IP addresses associated with a sample of jumpbox servers and ascertained that the IP addresses allocated were restricted to a specific subnet for each instance of Azure cloud. • Obtained and inspected configuration for a sample of network devices and ascertained that device access was restricted via above terminal servers.	
OA - 14	Access to network devices in the scope boundary requires two-factor authentication and / or other secure mechanisms.	• Inquired of management if two-factor authentication is enforced for connecting to a network device. • For a sampled network device, observed that logging in to the network device required two-factor authentication. • Obtained and inspected configuration for a sample of network devices, and ascertained that authentication was enforced via TACACS+ servers.	No exceptions noted.
OA - 15	Passwords used to access Azure network devices are restricted to authorized individuals based on job responsibilities and changed on a periodic basis.	• Inquired of management to gain an understanding of how passwords used to access network devices are restricted and rotated. • Obtained and inspected tickets / rotation logs for sampled network devices to ascertain that the passwords for network devices were rotated as per the defined cadence. • Observed that passwords were stored in secret repositories with access restricted to authorized individuals based on job responsibilities.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
OA - 16	Network filtering to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted service components is implemented.	• Inquired of management regarding the packet filtering mechanisms implemented to restrict incoming and outgoing traffic. • Obtained and inspected the configuration files for a cluster within the sampled datacenters and ascertained that filtering mechanisms and rules were configured to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted service components.	No exceptions noted.
OA - 17	External traffic to the customer VM(s) is restricted to customer - enabled ports and protocols.	• Inquired of management regarding network access controls in place to restrict external traffic to ports and protocols defined and enabled by customers. • Attempted to access a sample set of VMs and observed that access was restricted based on the external traffic rules for ports and protocols enabled within the service configuration.	No exceptions noted.
OA - 18	Azure network is segregated to separate customer traffic from management traffic.	• Inquired of management regarding the procedures and technical controls used for segregating networks within the Azure environment. • Obtained and inspected mechanisms used for segregating and restricting network traffic within the Azure environment.	No exceptions noted.
OA - 19	Microsoft Azure has published virtualization industry standards supported within its environment.	• Inquired of management to understand the various published virtualization industry standards supported within the Azure environment, and solution-specific virtualization hooks available for customer review. • Reperformed the control to ascertain that Azure published virtualization formats (e.g., Open Virtualization Format (OVF)) supported interoperability with third-party products.	No exceptions noted.
OA - 20	Alerts are generated when a break-glass account is used to access a production subscription.	• Inquired of management to understand the procedures in place for monitoring break-glass account access to the production environment.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		• 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.	
OA - 21	Access to production resources requires the use of a Secure Admin Workstation (SAW) which requires MFA for access.	• Inquired of 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.	No exceptions noted.
DS - 1	Cryptographic certificates, keys, and customer access keys used for communication between Azure services and other internal components are stored securely and are rotated on a periodic basis.	• Inquired of management to understand the different types of cryptographic certificates and keys used by the services to connect to internal components, and their cadence / frequency of rotation. • Observed the security of the cryptographic certificates and keys, and the process for periodic rotation. Additionally, ascertained through inspection of security group membership that the security groups granting access to the secrets were restricted to those personnel having valid business justification for access. • For a sample of services, obtained and inspected evidence (e.g., tickets, logs) indicating if the secrets were rotated based on the pre-determined frequency. • Performed inquiry and ascertained that the master key was secured based on controlled procedures.	**Exception noted:** Three of 24 sampled secrets tested during the period 4/1/2024 to 12/31/2024 were not rotated as per the secret rotation cadence defined in the documented procedures. Further, tested 11 sampled secrets subsequent to December 31, 2024, and no additional exceptions were noted. Additionally, certain internal Microsoft platform keys were not rotated according to the prescribed cadence outlined in the internal policy. As mitigation, these keys were protected through other security practices, including additional encryption.

Control ID	Control Activity	Test Procedures	Results of Tests
			Separately, as part of its investigation into the actions of Midnight Blizzard, Microsoft identified passwords and secrets impacting certain in-scope Azure services that were accessed by the threat actors through code repositories or Microsoft corporate email. Furthermore, Internal Audit of Microsoft identified multiple secrets associated with four in-scope services that were not rotated during the past year.
DS - 2	Customer data communicated through Azure service interfaces is encrypted during transmission over external networks. Location-aware technologies are implemented within the Azure portal to identify and validate authentication sessions.	• Inquired of management to understand the controls in place that restrict transmission of customer data to secure protocols through various endpoints over external networks, and location-aware technologies which are implemented within the Azure Portal. • Reperformed the control to ascertain that restrictions were in place to prevent use of insecure protocols (e.g., HTTP) for transmission of customer data over external networks, and location-aware technologies were implemented within the Azure Portal to identify and validate authentication sessions.	No exceptions noted.
DS - 3	Internal communication between key Azure components where customer data is transmitted / involved is secured using encryption.	• Inquired of management to understand the use of secure mechanisms such as encryption for communication between internal Azure components that involves customer data. • For a sample of Azure platform components, inspected configurations and observed the use of secure encryption mechanisms for internal communication.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
DS - 4	Cryptographic controls are used for information protection within the Azure platform based on the Azure Cryptographic Policy and Key Management procedures. The policies and procedures include the key rotation, archival and deactivation processes. Keys must have identifiable owners (binding keys to identities) and key management policies.	• Inquired of management regarding the policies and procedures in place for using cryptographic controls within the Azure environment. • For a sample of services, inspected work items to ascertain that cryptographic policy requirements were enforced. • For a sample of secrets from different Azure services, obtained and inspected secret configuration to ascertain that secrets were stored under service specific vaults or configuration files.	No exceptions noted.
DS - 5	Backups of key Azure service components and secrets are performed regularly and stored in fault-tolerant (isolated) facilities. Backups are monitored and backup errors are investigated and followed-up on appropriately.	• Inquired of management if backups of key Azure service components and secrets are performed regularly and stored in fault tolerant facilities. • Obtained and inspected configurations and logs to ascertain that platform data and secrets data were replicated, backed up, and stored in separate locations. • Obtained and inspected sample IcM tickets generated to ascertain that backup errors were investigated and remediated appropriately.	No exceptions noted.
DS - 6	Critical Azure components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services.	• Inquired of management about the redundancy mechanisms in place for key components within the production environment. • For a sample of platform components, inspected configurations and ascertained that redundancies were implemented within the production environment.	No exceptions noted.
DS - 7	Customer data is automatically replicated within Azure to minimize isolated faults. Customers are able to determine geographical regions of the data	• Inquired of management about the redundancy mechanisms in place to replicate data stored across Azure services. • For a sample of services, inspected the data replication configuration settings and ascertained that data was replicated across multiple nodes.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	processing and storage, including data backups.	- Obtained and inspected configurations for the sampled services to determine geographical region of the data processing and storage.	
DS - 8	Data Protection Services (DPS) backs up data for properties based on a defined schedule and upon request of the properties. Data is retained according to the data type identified by the property. DPS investigates backup errors and skipped files and follows up appropriately.	- Inquired of management regarding the process for scheduling of backups of production database based on customer requests. - Inquired of management if backup of customer data was performed based on a defined schedule in accordance with documented operating procedures. Additionally, inspected the procedures to ascertain that retention of backup data was consistent with the security categorization assigned to it. - For a sample of backup scheduling requests, obtained and inspected backup logs and ascertained that they were completed in accordance with customer requests and documented operating procedures. For a sample of backup failures, obtained tickets / backup status showing resolution details.	**Exception noted:** Management identified a vulnerability in the supporting third-party software used in scheduling of their internal offline backups. As a result, management paused backups, resulting in the control not operating effectively from February 22, 2025.
DS - 9	Backup restoration procedures are defined and backup data integrity checks are performed through standard restoration activities.	- Inquired of management if backup data integrity checks are conducted as part of standard restoration activities. - Obtained and inspected DPS operating procedures and ascertained that processes for completing restoration from backups were defined. Additionally, ascertained that a ticketing system was used for tracking restoration requests. - For a sample of restoration requests, obtained and inspected restoration tickets to ascertain that backup data integrity checks were completed in accordance with the request and documented operating procedures.	**Exception noted:** Management identified a vulnerability in the supporting third-party software used in scheduling of their internal offline backups. As a result, management paused backups, resulting in the control not operating effectively from February 22, 2025.
DS - 10	Guidelines for the disposal of storage media have been established.	- Inquired of management to understand the process for disposal of storage media.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		• Obtained the population of storage media disposals performed during the examination period, and judgmentally selected a sample of disposals. For a sample of media disposal requests, obtained and inspected evidence (destruction certificates) to ascertain that they followed the standard disposal process.	
DS - 11	Data corresponding to Azure is backed up to another region other than the primary data location and retained as per the retention policy.	• Inquired of management if processes for backups and retention to primary and secondary locations are established. • Obtained the total population of storage policies. Selected a sample of storage policies, and obtained and inspected their backup and retention policy configuration, to ascertain that data is backed up and retained as per the retention policy.	**Exception noted:** Management identified a vulnerability in the supporting third-party software used in scheduling of their internal offline backups. As a result, management paused backups, resulting in the control not operating effectively from February 22, 2025.
DS - 13	Production data on backup media is encrypted.	• Inquired of management if production data is encrypted prior to storage on backup media. • For a sample of Azure blob servers, obtained and inspected data encryption configurations to ascertain that production data was encrypted. • Obtained and inspected the configuration settings for a sample of backup encryption system instances to ascertain whether they are enabled to encrypt production data for tape backups.	No exceptions noted.
DS - 14	Azure services are configured to automatically restore customer services upon detection of hardware and system failures.	• Inquired of management about the failover mechanisms in place to automatically restore role instances upon detection of a hardware and system failure. • For a sample of node instances, observed the health status and service healing history to ascertain that automatic restoration was occurring.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
DS - 15	Customer data is retained and removed per the defined terms within the Product Terms, when a customer's subscription expires, or is terminated.	• Inquired of management about the policy and procedures in place for the removal / retention of customer data upon termination of subscription. • Obtained and inspected customer documentation to ascertain that data removal / retention processes were addressed. • For a sampled subscription, ascertained that access to customer data was handled in accordance with Product Terms upon termination of the subscription.	No exceptions noted.
DS - 16	Each Online Service's customer's data is segregated from other Online Services' customers' data, either logically or physically.	• Inquired of management to understand how the AAD Distributed Directory Services environment enforces logical or physical segregation of customer data. • Reperformed the control using test domains to ascertain that customer (tenant) data was segregated.	No exceptions noted.
DS - 17	Azure provides customers the ability to manage their own data encryption keys.	• Inquired of management regarding the policies and procedures in place for customers to manage their own data encryption keys within the Azure environment. • Obtained and inspected the policy and procedure documentation to ascertain that the processes are in place for the customers to manage their own encryption keys. • Reperformed the procedures in an Azure tenant to ascertain that customers are able to manage their own encryption keys.	No exceptions noted.
DS - 18	Microsoft performs a risk assessment for encryption and key management to evaluate changes and updates to cryptography controls.	• Inquired of management on the policy and procedures in place for performing the risk assessments for changes and updates to encryption, key management and cryptography controls. • Obtained and inspected meeting invites and meeting minutes of sampled crypto board meetings to ascertain that risk assessment is performed for changes identified for encryption, key management and cryptography controls.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
CM - 1	Procedures for managing different types of changes, including emergency changes, to the Azure platform have been documented and communicated.	• Inquired of management regarding the procedures for managing various types of changes to the Microsoft Azure environment including tracking, approval, and testing requirements. • Obtained documentation of Change Management procedures. Inspected documentation and ascertained that procedures for requesting, classifying, approving and implementing all types of changes, including major release, minor release, hotfix, and configuration changes, were defined.	No exceptions noted.
CM - 2	Secondary approval is required prior to all pull request check-ins to the production build, enforcing segregation among designated personal when implementing changes.	• Inquired of management if segregation of duties for key responsibilities for requesting, approving, and implementing changes to the Azure platform, is implemented. • Identified and obtained the population of production deployments made during the examination period from the ticketing system, for the Microsoft Azure platform. • Selected a sample of changes to production and ascertained that key responsibilities were segregated.	**Exception noted:** Management self-identified a vulnerability that could have allowed a single individual to submit and approve code bypassing SOD controls at the pull request level by using two user accounts owned by the same individual (i.e. Corp and Alt accounts). Management identified and disclosed 31 related instances from a large quantity of pull requests where developers self-approved their pull requests before checking them into the production build, leveraging multiple user accounts that they owned. Additionally, tested 15 change samples subsequent to September 30, 2024 and no

Control ID	Control Activity	Test Procedures	Results of Tests
			additional exceptions were noted.
CM - 3	Key stakeholders approve prior to deploying a release into production based on documented change management procedures.	• Inquired of management about the procedures for managing various types of changes to the Microsoft Azure environment, including approval requirements. • Identified and obtained the population of production deployments made during the examination period from the ticketing system, for the Microsoft Azure platform. • Selected a sample of changes to production and ascertained that documented procedures for approval (including if the result of the risk assessment is documented appropriately and comprehensively and all changes were prioritized on the basis of the risk assessment) were followed prior to deployment.	No exceptions noted.
CM - 4	Software releases and configuration changes to the Azure platform are tested based on established criteria prior to production implementation.	• Inquired of management about the procedures for managing various types of changes to the Microsoft Azure environment, including testing requirements. • Identified and obtained the population of the production deployments made during the examination period from the ticketing system, for the Microsoft Azure platform. • Selected a sample of changes to production and ascertained that documented procedures for testing were followed prior to deployment.	No exceptions noted.
CM - 5	Implemented changes to the Azure platform 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.	• Inquired of management regarding the procedures for reviewing implemented changes for adherence to established procedures prior to closure. • Identified and obtained the population of production deployments made during the examination period from the ticketing system, for the Microsoft Azure platform. • Selected a sample of changes to production and ascertained that roll back procedures were in place to roll back changes to their previous state in case of errors or security concerns.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		• Selected a sample of changes to production and ascertained that changes were reviewed prior to closure.	
CM - 6	Procedures to manage changes to network devices in the scope boundary have been established.	• Inquired of management regarding the procedures established for managing changes to network devices in the scope boundary. • Inspected network change management procedures, and for a sample of changes, obtained and inspected change management tickets to ascertain that documented procedures for managing changes to network devices including documentation, classification, review, testing and approval, were followed prior to deployment.	No exceptions noted.
CM - 7	Secure network configurations are applied and reviewed through defined change management procedures.	• Inquired of management if the implementation and review of secure network configuration standards are followed through defined change management procedures. • Inspected network configuration change management procedures and tested if change management procedures for secure network configuration changes were established. • Obtained and inspected a sample of network change requests and ascertained that changes were documented, tested, reviewed, and approved based on the change type.	No exceptions noted.
CM - 8	The Technical Security Services team develops security configuration standards for systems in the physical environment that are consistent with industry-accepted hardening standards. These configurations are documented in system baselines, are reviewed annually, and relevant configuration changes are communicated to impacted teams.	• Inquired of management if security configuration standards for systems in the datacenters' environment are based on industry-accepted hardening standards and configurations are documented in system baselines and are reviewed annually. Relevant configuration changes are communicated to impacted teams. • Inspected security configuration standards and technical baseline published in a central location and approvals related to an annual review and ascertained that technical baselines were consistent with the industry standard, approved, and the results were communicated to impacted teams.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		• Selected a sample of servers and inspected their configuration to ascertain that documented security configuration standards and technical baseline were implemented.	
CM - 9	Datacenter change requests are classified, documented, and approved by the Operations Management Team.	• Inquired of management if change requests are classified, documented, and approved by the Operations Management Team. • Inspected procedures and tested if established procedures cover the process for requesting, documenting (including if the changes were assessed for risk and prioritized), classifying, approving, and executing datacenter changes. • Selected a sample of change requests and tested that changes were classified, approved, and executed in accordance with documented procedures.	No exceptions noted.
CM - 10	Secure configurations for datacenter software are applied through defined change management procedures including documentation, testing and approval.	• Inquired of management if server-based images are documented, tested and approved. Additionally, inquired if release to production is restricted to appropriate personnel. • Obtained and inspected user access to the release production server and ascertained that access was restricted to appropriate personnel. • Selected a sample of bugs and requirements from the releases during the period and inspected change tickets to ascertain that secure configurations for datacenter software were applied through defined change management procedures.	No exceptions noted.
CM - 12	Azure has implemented tools to perform integrity verification checks to detect unauthorized changes to software, firmware and information.	• Inquired of management regarding the tools implemented to detect unauthorized changes to software, firmware and information. • For a sample of code integrity alerts, obtained and inspected logs and ascertained that the changes were identified by unique event IDs, and appropriate teams were notified to investigate and resolve identified items.	**Exception noted:** For the period April 1, 2024 to March 31, 2025, Internal Audit Team of Microsoft noted that code-signing was not configured for seven of the build pipelines associated with five of the in-scope services.

Control ID	Control Activity	Test Procedures	Results of Tests
			No additional exceptions were noted in our independent testing.
CM - 13	Any changes to production via break-glass have been reviewed to ensure all changes were appropriate. Management monitors break-glass alerts on periodic basis to ensure that alerts are appropriately reviewed.	• Inquired of management to gain an understanding of the process related to performing review of changes made through break-glass accounts in the production environment. • For all break-glass account access scenarios during the examination period, obtained and inspected tickets to ascertain that access was reviewed for appropriateness. • For a sample of months, obtained and inspected evidence of monthly review of break-glass alerts by management to ascertain that break-glass alerts are appropriately reviewed by management.	No exceptions noted.
SDL - 1	Development of new features and changes to the Azure services follow a defined approach based on the Microsoft Security Development Lifecycle (SDL) methodology. The SDL review for each service is performed on an annual basis.	• Inquired of management if the Microsoft SDL methodology for the development of new features and changes to Microsoft Azure services is defined. • Obtained and inspected documentation to ascertain that SDL methodology was defined to incorporate security and privacy practices as part of the development process. • For a sample of Azure services, obtained and inspected evidence to ascertain that the SDL review was conducted on an annual basis and that the defined approach for development of new features and changes was followed based on the Microsoft SDL methodology.	**Exception noted:** For 15 of the 36 sampled services, SDL review was not completed within the annual cadence. For the period 04/01/2024 to 08/31/2024, Internal Audit of Microsoft identified one additional sample that did not meet the annual SDL review cadence. Additionally, Internal Audit of Microsoft identified one sampled service in which two exceptions were not approved timely and by the appropriate personnel as per Microsoft's SDL Methodology.

Control ID	Control Activity	Test Procedures	Results of Tests
SDL - 2	Applicable operational security and internal control requirements are documented, and implemented for Azure services based on Microsoft SDL methodology.	• Inquired of management to gain understanding of the process to identify and document applicable operational security and internal control requirements as part of the SDL methodology. • For a sample of Azure services ascertained that operational security and internal control requirements were documented and implemented as per the Microsoft SDL methodology.	No exceptions noted.
SDL - 3	Responsibilities for submitting and approving production deployments are segregated within the Azure teams.	• Inquired of management if responsibilities for production deployment are segregated within the Microsoft Azure teams. • For a sample of services, inspected access control lists to ascertain that segregation was maintained within the teams for submitting and approving production deployments and that the access to perform production deployments was restricted to authorized individuals within the Azure teams.	No exceptions noted.
SDL - 4	New features and major changes are developed and tested in separate environments prior to production implementation. Production data is not replicated in test or development environments.	• Inquired of management if changes are developed and tested in separate environments prior to production deployment and production data is not replicated in test or development environments. • For a sample of services, obtained and inspected subscription namespaces to ascertain that separate environments existed for development and testing of changes prior to production deployment. • For the sampled services, inquired of service owners and inspected policies, test scripts, or configuration files, as applicable, to ascertain that production data is not replicated to the test or development environments. • For a sample of changes made to production, obtained and inspected tickets to ascertain that documented procedures for testing were followed prior to deployment.	No exceptions noted.
SDL - 5	Azure Services use code repositories for managing source code changes. Procedures to	• Inquired of management about the procedures established to manage changes to source code stored in a repository.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	approve code changes managed through source code repository are established. Code changes submitted to the repository are logged and can be traced to the individuals or system components executing them.	• For a sample of services, obtained and inspected the branch policy settings and associated membership details to ascertain that source code changes are approved by appropriate personnel. • For a sample source code repository, observed 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 are logged.	
SDL - 6	Source code builds are scanned for malware prior to release to production.	• Inquired of management regarding the procedures in place to scan source code builds for malware. • 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.	No exceptions noted.
VM - 1	Azure platform components are configured to log and collect security events.	• Inquired of management regarding security event logging configured for Azure services to enable detection of potential unauthorized or malicious activities. • Inspected alert configurations and a sample notification for a sampled server to corroborate that security events generated alerts based on defined rulesets. • For a sample of servers, obtained and inspected security logs to ascertain that logging of key security events was enabled per documented procedures. • Observed the security event monitoring configuration for a sampled server to ascertain that a mechanism was in place to detect and restart the logging process in case of disconnectivity.	No exceptions noted.
VM - 2	Administrator activity in the Azure platform is logged.	• Inquired of management regarding the mechanisms that are in place for logging administrator activities within Azure Service platform.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		• For a sample of services, obtained and inspected security logs to ascertain that administrator events were logged to the centralized monitoring infrastructure.	
VM - 3	A monitoring system to monitor the Azure platform for potential malicious activity and intrusion past service trust boundaries has been implemented.	• Inquired of management regarding the monitoring capabilities within the Azure environment to detect potential malicious activities and intrusions. • For a sample of servers, inspected logs to ascertain that malicious activities were monitored as per the process. • Additionally, inspected anti-malware event logging and the status of anti-malware engine signatures for a sample of servers to corroborate that they were up to date.	No exceptions noted.
VM - 4	Procedures to investigate and respond to malicious events detected by the Azure monitoring system in a timely manner have been established.	• Inquired of management to ascertain that incidents and malicious events are identified, tracked, investigated, and resolved in a timely manner per documented procedures. • Obtained and inspected a sample of incident tickets pertaining to the Azure Services and ascertained that incidents and malicious events were monitored, identified, tracked, investigated, and resolved.	No exceptions noted.
VM - 5	Procedures to evaluate and implement Microsoft-released patches to Service components have been established.	• Inquired of management regarding the patch management process within the Azure environment. • Inspected patch management SOP and ascertained that procedures for evaluating and implementing relevant security patches within the Azure environment were established. • For a sample of servers, obtained and inspected logs and patch details to ascertain that a selection of patches was assessed and implemented into the production environment per documented procedures.	No exceptions noted.
VM - 6	Procedures to monitor the Azure platform components for known security vulnerabilities have been	• Inquired of management if processes to monitor and remediate known security vulnerabilities on the Azure platform are in place.	**Exception noted:** Internal Audit of Microsoft identified multiple vulnerabilities associated with

Control ID	Control Activity	Test Procedures	Results of Tests
	established. Identified security vulnerabilities are remediated.	• Obtained and inspected the Vulnerability Risk Management SOP and ascertained that procedures for scanning and remediating vulnerabilities identified on servers have been established. • For a sample of Azure platform components, obtained and inspected scan results to ascertain the components were monitored for security vulnerabilities. Furthermore, inspected the scan results and ascertained that, if vulnerabilities were identified during the sampled months, they were remediated within the defined timelines.	five in-scope services that were not remediated in a timely manner within the expected SLA. No additional exceptions were noted in our independent testing.
VM - 7	Procedures to configure and monitor network devices in the scope boundary, and resolve issues, have been established.	• Inquired of management to ascertain that procedures for configuring and monitoring network devices in the scope boundary are established, and that identified issues are resolved. • Obtained and inspected documentation and ascertained that procedures related to network infrastructure were established and included network device access, configuration management, network device change management, Access Control List (ACL) change management, and ACL triage process. Additionally, ascertained that the procedures were reviewed by the Networking team management on an annual basis.	No exceptions noted.
VM - 8	Penetration testing of critical infrastructure components is performed at least annually based on documented Penetration testing procedures and findings are documented, tracked, and remediated.	• Inquired of management regarding the procedures established to perform penetration testing on the Azure environment. • Obtained and inspected the contractual agreements and results of the latest penetration testing performed on the Azure environment to ascertain: – Penetration testing was performed by internal personnel or external service providers at least annually – Critical infrastructure components were included in the scope boundary	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		– Findings were documented, tracked and remediated for critical and high severity	
VM - 9	Network devices in the scope boundary are configured to log and collect security events, and monitored for compliance with established security standards.	• Inquired of management to ascertain that network devices in the scope boundary are configured to log and collect security events, and monitored for compliance. • For a sample of network devices in the scope boundary, obtained and inspected device configurations to ascertain that they were configured to log and collect security events, with event logs routed to designated log servers. • Inspected configuration compliance reports for the sampled network devices, and ascertained that scans were configured per established security standards. For devices identified by scanning as not being in compliance, ascertained that issues were investigated and resolved.	No exceptions noted.
VM - 10	Azure provides logging mechanisms that can be configured by customers to log activities and performance metrics.	• Inquired of 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 performance metrics. Inspected the logs available on the portal and ascertained that expected entries are being logged.	No exceptions noted.
VM - 11	Microsoft operating system updates for virtual machines are made available through Microsoft Security Response Center (MSRC) site and Windows Update.	• Inquired of management regarding the mechanisms to update the Microsoft operating system installed on virtual machines through the Microsoft Security Response Center (MSRC) and Windows Update.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		• Inspected the MSRC to ascertain that updates to the Microsoft operating system on virtual machines are available through the MSRC. Accessed Windows Update and observed that customers can configure virtual machines to update operating systems as needed. Reperformed by configuring automatic updates and through inspection ascertained that updates were applied as a result.	
VM - 12	The availability of Azure services is monitored through third-party and internal tools, and the status is communicated through a Service Dashboard.	• Inquired of management to understand the processes followed and tools used by the services for monitoring service availability and communicating service availability status to customers through Service Dashboard. • For a sample of services, inspected monitoring tools and configurations to ascertain that the availability tools were implemented to monitor service availability and generate real-time alerts to notify the designated personnel of any issues. • Inspected the Service Dashboard to ascertain the availability status of services were accurately reflected.	No exceptions noted.
VM - 13	Vulnerabilities for network devices are evaluated and mitigated based on documented procedures.	• Inquired of management if documented procedures are followed when remediating vulnerabilities on network devices. • Obtained and inspected documentation to ascertain if procedures to evaluate vulnerability risks have been established. • Selected a sample of vulnerabilities for the respective network devices and inspected the corresponding remediation procedure to ascertain if applicable and defined mitigation procedures were implemented.	No exceptions noted.
IM - 1	An incident management framework with defined processes, roles, and responsibilities for the detection, escalation and response of incidents, has been established and communicated.	• Inquired of management if information security incidents are managed through designated responsibilities and documented procedures.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		• Obtained and inspected information security incident management procedures and ascertained that roles and responsibilities for escalation and notification to specialist groups during an incident were established and communicated.	
IM - 2	Events, thresholds, and metrics have been defined and configured to detect incidents and alert the associated Operations team.	• Inquired of management if events, thresholds and metrics are established to detect and facilitate an alert / notification to incident management teams. • Observed the configuration files and ascertained that automated monitoring and notification was configured for predefined events. • For a sample of platform components, ascertained that automated notifications were received upon the occurrence of an event meeting the configured specifications.	No exceptions noted.
IM - 3	The Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures.	• Inquired of management about the procedures for 24x7 monitoring and handling of incidents. • Identified the population of incidents in the examination period and obtained and inspected a sample of incident tickets to ascertain that each incident was handled per documented procedures. • Inspected a sample of incident tickets and ascertained that there is monitoring of alerts and notification of potential incidents. • Obtained and inspected Monitoring team schedules to ascertain that there was 24x7 monitoring.	No exceptions noted.
IM - 4	Incident post-mortem activities for severe incidents impacting the Azure environment are conducted.	• Inquired of management if a post-mortem is performed for customer impacting severity 0 and 1 incidents and a formal report is submitted for management review and that mechanisms are in place to track and remediate recurring incidents. • Inspected a sample of incidents to ascertain that post-mortem was performed as per documented procedures.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
IM - 5	The Cyber Defense Operations (CDO) team provides reports of information security events to Cloud + AI management on a quarterly basis. Problem statements for systemic issues are submitted to executive leadership for review.	• Inquired of management if information security review report is presented to Cloud + AI management on a quarterly basis. • Obtained and inspected a sample of quarterly reports and ascertained that problem statements for systemic issues were submitted for executive leadership review. • Obtained and inspected evidence (such as meeting invite, list of attendees) to ascertain that the report was reviewed by executive leadership.	No exceptions noted.
IM - 6	The Cyber Defense Operations (CDO) team performs annual tests on the security incident response procedures.	• Inquired of management if incident response procedures are tested at least annually and the test results are documented in centralized tracking system. • Obtained and inspected the documentation from the exercise conducted by the CDO team including the test plan and testing results and noted that the tested action items, expected results, and actual results were included and documented.	No exceptions noted.
PE - 1	Procedures to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors, have been established.	• Inquired of management if access levels are established and if physical access to the datacenter is restricted to authorized personnel. • Inspected the datacenter SOPs and ascertained that procedures were in place to restrict physical access to the datacenter for employees, vendors, contractors, and visitors. Inquired of management regarding the review and communication of the procedures. • Obtained and inspected a sample of access requests and ascertained that access requests were tracked using a centralized ticketing system and were authorized by the designated approvers.	No exceptions noted.
PE - 2	Security verification and check-in for personnel requiring temporary access to the interior of the	• Inquired of management if security verification and check-in procedures are established for personnel requiring temporary access to the interior datacenters.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	datacenter facility, including tour groups or visitors, are required.	• Inspected the datacenter SOPs and ascertained if procedures were in place for security verification, check-in, and escorting personnel requiring temporary access to the interior of the datacenter facility, including tour groups or visitors.	
PE - 3	Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team.	• Inquired of management if physical access to datacenters is reviewed and verified quarterly. • Inspected Datacenter Services (DCS) operating procedures and ascertained that quarterly access review procedures were documented. • For sampled quarterly access reviews, ascertained that reviews were completed appropriately.	No exceptions noted.
PE - 4	Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.	• Inquired of management if physical access mechanisms to restrict access to authorized individuals are in place. • For a sample of datacenters, observed that access to the main entrance of the datacenter, exterior doors, co-locations, and other interior rooms within the datacenter was restricted through physical access mechanisms (such as electronic card readers, biometric handprint readers, or man traps). • Observed attempts to access restricted areas within the datacenters without appropriate level of access and ascertained that access was denied.	**Exception noted:** For 1 of 17 sampled datacenters, while there are various layers of physical access mechanisms that were determined to be properly implemented, two instances of physical access mechanisms were not properly administered: - A trash door that provides access to the loading area was not fully closed. - While keycards were required to enter the generator area, several generator enclosures within the area that are normally secured with temporary-use

Control ID	Control Activity	Test Procedures	Results of Tests
			physical keys had broken or unsecured locks.
PE - 5	The datacenter facility is monitored 24x7 by security personnel.	• Inquired of management if security personnel monitor the datacenter premises through a video surveillance system 24 hours a day, 7 days a week. • Observed security personnel as well as video surveillance systems at a sample of datacenters and ascertained that views for facility entrances, exits, parking lots, doors, co-locations, restricted areas and / or loading / delivery docks were being monitored by security personnel using on-site security consoles. • Requested surveillance tapes for a sample of datacenters and inspected that the tapes were retained according to the documented operating procedures.	**Exception noted:** For 1 of the 32 sampled cameras, the tapes were not retained in accordance with the documented operating procedures.
PE - 6	Datacenter Management team maintains and tests datacenter-managed environmental equipment within the facility according to documented policy and maintenance procedures.	• Inquired of management if environmental equipment within datacenter facilities is maintained and tested according to documented policy and maintenance procedures. • Inspected DCS operating procedures and ascertained that procedures were documented for maintaining adequate facility and environmental protection at the datacenters. • For a sample of datacenters observed that the critical environment was being monitored. • Inspected maintenance and testing records for a sample of on-site environmental equipment.	No exceptions noted.
PE - 7	Environmental controls have been implemented to protect systems inside datacenter facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and	• Inquired of management if environmental controls are implemented to protect systems inside the datacenters. • For a sample of datacenters, observed that environmental controls including temperature control, HVAC (heating, ventilation and air conditioning), fire detection and suppression systems, and power management systems were in place.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	suppression systems, and power management systems.		
PE - 8	Datacenter physical security management reviews and approves the incident response procedures on a yearly basis. The incident security response procedures detail the appropriate steps to be taken in the event of a security incident and the methods to report security weaknesses.	• Inquired of management if an incident response procedure is established to address physical security incidents and methods to report security incidents, and these are reviewed and approved annually. • Inspected the Incident Response Procedure and ascertained that the procedure was approved by appropriate Physical Security Managers and included documentation of severity of events, procedures to be followed in the event of a physical security incident and guidelines for emergency communication and reporting.	No exceptions noted.
LA - 1	External access to Azure services and the customer data stored in the service requires authentication and is restricted based on customer configured authorization settings.	• Inquired of management to understand the mechanisms implemented to allow customers to configure access or traffic restrictions. • Reperformed the control for a sample of services to ascertain that access to the service was restricted based on the customer configured authentication and authorization settings.	No exceptions noted.
LA - 2	Customer credentials used to access Azure services meet the applicable password policy requirements. Temporary credentials assigned to users by the service expire within 14 days and users are forced to change these credentials when using them for the first time.	• Inquired of management regarding controls in place to ascertain the following requirements: – New passwords within Azure conform to the applicable password policy requirements – Users are forced to change the password when using them for the first time – Temporary credentials assigned to users by the service expire within 14 days • Reperformed the control for a sample of services through various scenarios such as: – Providing sample weak passwords	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		– Tampering with the Hypertext Transfer Protocol (HTTP) request by using weak passwords – Using expired passwords to ascertain that new password(s) that did not meet applicable password policy requirements were not accepted.	
LA - 3	Logical segregation to restrict unauthorized access to other customer tenants is implemented.	• Inquired of management to understand the segregation controls implemented to restrict unauthorized access to other customer tenants. • Reperformed the control for a sample of services to ascertain that segregation was enforced between the tenants, and that customers could access the data within the service only after the required authorization checks.	No exceptions noted.
LA - 4	Customer data that is designated as “confidential” is protected while in storage within Azure services.	• Inquired of management to understand the controls implemented to protect customer confidential data stored within the service. • Reperformed the control for a sample of services to ascertain that customer confidential data stored within the service was protected.	No exceptions noted.
LA - 5	User sessions within Azure can be configured by customers to expire after a stipulated period of inactivity.	• Inquired of management to understand the mechanisms implemented to enforce session timeout. • Reperformed the control to validate that: – Sessions are invalidated after an idle timeout as configured by the user or tenant administrator – Session remains active if timeout is set to ‘never’ after a long duration	No exceptions noted.
LA - 6	The jobs configured by the customer administrators are executed within thirty (30) minutes of the scheduled job run and are	• Inquired of management to understand the mechanisms in place to execute jobs, configured by the customer administrators, within thirty (30) minutes of the scheduled job run and repeat based on the defined recurrence settings.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	repeated based on the defined recurrence settings.	• Reperformed the control for a sample job to ascertain that jobs configured by the customer administrators were executed within thirty (30) minutes of the scheduled job run and were repeated based on the defined recurrence settings.	
LA - 7	Quotas on Azure services are enforced as configured by the service administrators to protect against availability related issues.	• Inquired of management to understand the mechanisms in place that allow customers to implement quotas on the service. • Reperformed the control for a sample of services by accessing the Azure Management Portal using a subscription, and ascertained that quotas and rate limits were enforced as configured.	No exceptions noted.
LA - 8	The private root key belonging to the Azure services is protected from unauthorized access.	• Inquired of management regarding the controls in place to protect the private root key, belonging to Azure services, from unauthorized access. • Obtained and inspected security plan for the physical location where private root keys are stored to ascertain that security procedures were established to protect the root key from unauthorized logical or physical access. • For a sample of access requests to the root key, obtained access notification and approval to ascertain that access to root keys were authorized and approved.	No exceptions noted.
LA - 9	Service initializes the resource groups within the management portal based on the customer configured templates. Service allows customers to monitor and control the distribution of system resources created within the resource group in order to prevent resources from being congested.	• Inquired of management to understand the mechanisms in place to initialize resource groups within the Azure Management Portal based on the customer configured templates and the mechanisms in place to monitor and control the distribution of the system resource created within the resource group. • Reperformed the control using a subscription and ascertained that the service was initialized based on customer configured templates.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		• Reperformed the control to ascertain that the distribution of the system resource created within a resource group can be monitored and controlled by customers.	
LA - 10	The errors generated during the job execution are monitored and appropriate action is taken based on the job settings defined by the customer administrator.	• Inquired of management regarding monitoring of errors generated during the job execution and actions taken based on the job settings defined by the customer administrator. • Reperformed the control for a sample of services to ascertain that errors generated during the job execution were monitored and actions were taken based on the job settings defined by the customer administrator.	No exceptions noted.
LA - 11	One Time Passwords (OTPs) used for self-service password reset are randomly generated. OTPs expire after a pre-defined time limit. OTPs sent to the customer administrator are required to be validated before a password change is allowed. SSPR does not display user identifiable information during the password reset. Microsoft Entra ID password policy requirements are enforced on the new passwords supplied by customer administrators within SSPR portal. New passwords supplied by customer administrators are protected during transmission over external networks.	• Inquired of management regarding the controls in place that: – Facilitate random generation of OTPs – Expire OTPs after their usage or after a pre-defined time limit – Validate the OTPs before the password is reset – Restrict transmission of new passwords to secure protocols through various endpoints over external networks – Validate if new passwords within the SSPR portal conform to the Microsoft Entra ID password policy requirements • Reperformed the control and obtained sample SMS and email OTPs to ascertain that the characters in the SMS and email were random. • Reperformed the control for various scenarios such as: – Reusing OTP after initially using it to reset passwords – Using OTP after expiration of the pre-defined time limit to ascertain that OTPs expired after a pre-defined time limit, and OTPs sent to the customer administrator were required to be validated before password was allowed to be changed.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		• Reperformed the control to ascertain that restrictions were in place to prevent use of insecure protocols (e.g., HTTP) for transmission of new passwords over external networks. • Reperformed the control through various scenarios such as: – Providing sample weak passwords through portal to ascertain that new passwords that did not meet necessary password policy requirements were not accepted by the SSPR portal.	
LA - 12	Images may be customized and access to images may be restricted by the customer. Updates to available images are communicated to through customer-facing websites.	• Inquired of management to understand how image access can be restricted, customized, and how updates are communicated to customers. • Reperformed the control by creating a customized image and restricting access to the image through the Azure portal. • Inspected communications of updates on customer-facing websites and also inspected the Azure Marketplace and ascertained that a selection of hardened images was available.	No exceptions noted.
ED - 1	Production servers that reside in edge locations are encrypted at the drive level.	• Inquired of management to gain an understanding of the encryption mechanism present at the drive level on production servers. • For a sample of production servers, ascertained that BitLocker was running and the Trusted Platform Module (TPM) was enabled.	No exceptions noted.
ED - 2	Intrusion alerts are sent to the operator when physical access to the production servers that reside in edge locations is detected.	• Inquired of management to understand the mechanism for detecting and alerting unauthorized physical access to production servers. • For a sample of production servers, obtained and inspected hardware specifications to ascertain that intrusion detection switches were present for the devices and inspected configurations to ascertain that they were enabled and configured to generate alerts upon detecting an intrusion.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
ED - 3	All unused IO ports on production servers that reside in edge locations are disabled through the configuration settings at the OS-level.	• Inquired of management to understand the configuration settings used to disable unused IO ports on production servers. • Obtained and inspected the configuration files for a sample of servers and ascertained that selected IO ports were disabled on the servers.	No exceptions noted.
BC - 1	Business Continuity Plans (BCP) for critical Azure services, which provide roles and responsibilities and detailed procedures for recovery and reconstitution of systems to a known state per defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), have been documented and published. Plans are reviewed on an annual basis, at a minimum.	• Inquired of management to understand the roles, responsibilities, and procedures established for developing business continuity plans, and recovery and reconstitution of systems per defined RTOs and RPOs. • For a sample of services, obtained and inspected the BCDR assessment reports and ascertained that RTOs and RPOs were documented, approved, and published for appropriate personnel. • Obtained and inspected the Business Continuity Plan (BCP) and ascertained that it was reviewed annually.	No exceptions noted.
BC - 3	Azure has developed a Business Continuity and Disaster Recovery (BC / DR) Standard Operating Procedure and documentation that includes the defined information security and availability requirements.	• Inquired of management to understand the processes in place for developing and maintaining Business Continuity and Disaster Recovery (BC / DR) Standard Operating Procedures (SOP). • Obtained and inspected the BC / DR SOP, and the overall business continuity plan to ascertain that information security and availability requirements were defined.	No exceptions noted.
BC - 4	The BCP team conducts testing of the business continuity and disaster recovery plans established for Azure services, per the defined testing schedule for different loss scenario. Each loss scenario is tested at least annually. Issues identified during testing are	• Inquired of management to understand the process in place for testing BC / DR plans. • For a sample of Azure services, obtained and inspected the BCDR assessment reports, including follow-up documentation for any issues identified and ascertained that BC / DR plans were established, reviewed, and tested at least annually.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	resolved and plans are updated accordingly.		
BC - 5	Risk assessments are conducted to identify and assess business continuity risks related to Azure services.	• Inquired of management to understand the processes in place for identifying and assessing the business continuity risks related to Azure services. • For a sample of services, obtained and inspected the Business Impact Analysis (BIA) and the Business Continuity Risk Assessment reports to ascertain that the business impact analysis was completed, and impact was assessed based on revenue and operational considerations.	No exceptions noted.
BC - 6	Procedures for continuity of critical services provided by third-parties have been established. Contracts with third-parties are periodically monitored and reviewed for inconsistencies or non-conformance. Procedures to transition between critical third-parties based on results of monitoring are established.	• Inquired of management to gain an understanding of the Service Level Agreements (SLAs) established for critical services provided by third parties. • Obtained and inspected the SLAs established for critical services provided by third parties, to ascertain that they were established, identified services to be performed, service levels to be provided, and established ownership of security processes. • For the sampled suppliers, obtained and inspected meeting notes and scorecards, as applicable, to ascertain that SLA monitoring was being performed. • Obtained and inspected documentation of exit strategy processes for critical service providers and suppliers to ascertain that procedures to transition between critical third parties were established.	No exceptions noted.
BC - 7	A Datacenter Business Continuity Management (BCM) program to respond to Microsoft's Enterprise Business Continuance Initiative has been implemented and includes documented procedures for mapping processes to pre-defined	• Inquired of management to understand the requirements established by Microsoft's Enterprise Business Continuity Management (EBCM) Program. • Obtained and inspected the Datacenter BCM program documents and ascertained that the Datacenter BCM program	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	enterprise functions, establishing recovery strategies as well as developing and conducting test scenarios that enable the BCM program to mitigate risks and vulnerabilities and respond to major disruptive events.	adhered to BCM PMO standards, methods, policies, and metrics.	
BC - 8	A Datacenter Business Continuity Management Program defines business continuity planning and testing requirements for functions within the datacenters. Datacenters exercise, test and maintain the Datacenter Business Continuity Plan for the continued operations of critical processes and required resources in the event of a disruption at least annually. The 'Business Continuity Management Exercise and Test Program Framework' document establishes the basis and process for exercising and testing of the plans for continuity and resumption of critical datacenter processes.	• Inquired of management if datacenters execute, test, and maintain Business Continuity Plans (BCPs) at least once a year. • Obtained and inspected the Business Continuity Management program documentation and ascertained that recovery strategies and procedures for resumption of critical business processes were documented and that the process for executing and testing of the plans for continuity and resumption of critical business processes were established. • For a sample of datacenters, obtained and inspected the GDCO tickets and ascertained that business continuity plans were tested as per the documented procedures.	No exceptions noted.
BC - 9	Datacenter Management teams conduct and document a resiliency assessment, specific to the datacenter's operations, on an annual basis or prior to proposed significant changes.	• Inquired of management to understand the datacenter resiliency assessment process and its cadence. • For a sample of datacenters, obtained the records of resiliency assessments conducted and ascertained that they were performed on an annual basis or prior to proposed significant changes.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
BC - 10	The network is monitored to ensure availability and address capacity issues in a timely manner.	• Inquired of management to understand the procedures established to monitor network capacity. • Obtained and inspected the capacity report for the sampled months to ascertain that the network availability was monitored and that capacity issues were addressed.	No exceptions noted.
PI - 1	Microsoft Azure monitors the transactions invoked by the customer and relays them appropriately to the suitable Resource Provider (RP) end-point. Actions are taken in response to defined threshold events.	• Inquired of management to ascertain that suitable measures are in place to monitor transactions invoked by the customer and relay them appropriately to Resource Provider (RP) end-points. • Obtained and inspected monitoring rules, and resulting notifications generated to check that errors in transactions were recorded and reported to required parties in a timely manner.	No exceptions noted.
PI - 2	Microsoft Azure management reviews portal performance monthly to evaluate compliance with customer SLA requirements.	• Inquired of management to ascertain that monthly review procedures are established to understand and evaluate portal performance against customer SLA requirements. • Obtained and inspected a sample of monthly scorecards, and ascertained that appropriate performance reviews were performed as per established procedures.	No exceptions noted.
PI - 3	Microsoft Azure performs input validation to restrict any non-permissible requests to the API.	• Inquired of management to understand mechanisms to perform input validation to restrict unauthorized access or non-permissible requests. • Reperformed the control to ascertain that invalid input provided by the user generated error messages for non-permissible requests.	No exceptions noted.
PI - 4	Microsoft Azure segregates and appropriately provisions the services based on request from customer through the portal / API.	• Inquired of management to understand mechanisms to perform request segregation and provision requested services to user accounts.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		- Reperformed the control to ascertain that service requests were segregated and provisioned based on subscription ID and other request parameters.	
SOC2 - 1	Azure assets are classified in accordance with Microsoft Online Services Classification Guidelines. The classification is documented, reviewed, and approved by the authorizing official.	- Inquired of management regarding the procedures related to the identification and classification of key information or data. - For a sample of services, obtained and inspected the current asset classification document and ascertained that it addressed the key data / information used by Microsoft Azure. Additionally, compared the asset classification to the Standard Operating Procedure (SOP) to ascertain whether it aligned with the approved definition criteria in the SOP.	No exceptions noted.
SOC2 - 2	Azure services maintain an automated inventory of key information assets. Automated quality control checks are implemented on all inventory data sources.	- Inquired of management on the process for maintaining and reviewing the inventory of key information or data. - For each asset inventory type, obtained and inspected the configuration files to ascertain that the inventory is complete and accurate. Additionally, noted that data quality control checks are enforced and alerting mechanisms are in place for any anomaly detected during the quality checks.	No exceptions noted.
SOC2 - 3	Datacenter team controls the delivery and removal of information system components through tickets on the Global Datacenter Operations (GDCO) ticketing system. Delivery and removal of information system components is authorized by system owners. System components / assets are tracked in the GDCO ticketing database.	- Inquired of management to gain an understanding of the process for delivery and removal of assets from datacenters. - Obtained the population of transports (both delivery and removal) performed during the examination period, and judgmentally selected sample transports. - For the sampled transports, obtained and inspected associated evidence (such as tickets, certificates) to ascertain that proper authorization was obtained prior to asset delivery and / or removal.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
SOC2 - 4	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.	• Inquired of 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.
SOC2 - 6	Azure maintains a Customer Support website that describes the process for customers and other external users to inform about potential security issues and submit complaints. Reported issues are reviewed and addressed per documented incident management procedures.	• Inquired of management regarding the Customer Support Website and the process for addressing reported customer incidents. • Observed Customer Support Website and ascertained that it allowed customers to report security issues or complaints. • Obtained the Incident Management (IcM) tickets for a sample to ascertain that each incident was handled per documented procedures. • Observed the Operations Center and ascertained monitoring of alerts and notification of potential incidents.	No exceptions noted.
SOC2 - 7	Azure 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.	• Inquired of management regarding the process for maintaining and communicating confidentiality and related security obligations for customer data, and recommendations for the secure use of cloud services to customers. • Inspected Microsoft Trust Center to ascertain that confidentiality and related security obligations were maintained and communicated to customers and observed that it included security related information and best practices for use of cloud services. • Obtained and inspected changes documented in Microsoft Trust Center to ascertain that changes related to the confidentiality	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		and related security obligations were communicated to customers.	
SOC2 - 8	Azure maintains and distributes an accurate system description to authorized users.	• Inquired of management regarding the procedures for the development, maintenance, and distribution of the system description. • Obtained Microsoft Azure service description and ascertained that it authoritatively described the system. • Observed that the service description was published and communicated to Microsoft Azure employees and relevant third-parties.	No exceptions noted.
SOC2 - 9	Azure maintains and notifies customers of potential changes and events that may impact security or availability of the services through an online Service Dashboard. Changes to the security commitments and security obligations of Azure customers are updated on the Azure website in a timely manner.	• Inquired of management regarding the process for notifying customers of security and availability events through the Service Dashboard. Additionally, inquired about the process for updating customers of changes to security commitments and obligations in a timely manner. • Observed the customer Service Dashboard and ascertained that it was updated with availability and customer events. • Selected a sample incident ticket to ascertain that the incident was reflected in the Service Dashboard’s history. • Observed the security commitments and obligations on the Microsoft Azure website and ascertained that they accurately reflected the security policies and procedures currently in place for the Microsoft Azure environment.	No exceptions noted.
SOC2 - 10	Prior to engaging in Azure services, customers are required to review and agree with the acceptable use of data and the Azure service, as well as security and privacy requirements, which are defined in the Product Terms, Microsoft Online	• Inquired of management regarding the procedures for the identification of security requirements and how customers must meet these requirements prior to gaining access to Microsoft Azure. • Obtained and inspected the End User Licensing Agreement (EULA) or Customer Agreements required by customers to sign	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	Subscription Agreement, Azure service Privacy Statement and Technical Overview of the Security Features in Azure service.	/ agree to prior to gaining access, and ascertained that they addressed identified security requirements. • Performed procedures to ascertain that agreements were required to be signed prior to subscription creation.	
SOC2 - 11	Microsoft has defined disciplinary actions for employees and contingent staff that commit a security breach or violate Microsoft Security Policy.	• Inquired of management that: – Disciplinary actions for employees and contingent staff, who commit a security breach or violate Microsoft Security Policy, have been established – The policy is communicated to the employees and relevant external parties • Obtained and inspected the HR policy and agreements, and ascertained that disciplinary actions were included for employees and contingent staff who commit a security breach or violate Microsoft Security Policy.	No exceptions noted.
SOC2 - 12	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.	• Inquired of management if procedures were established to perform background checks on new or transferred Microsoft personnel before they were granted access to data and assets. • Obtained and inspected procedures document to ascertain that background screening performed included verification of personal and professional history. • Obtained the total population of new hires from the HR system from the examination period. Selected a sample of new hires to ascertain that background checks were performed prior to access being granted to critical data / applications.	No exceptions noted.
SOC2 - 13	Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees are provided	• Inquired of management if Non-Disclosure Agreements (NDAs), that include asset protection and return responsibilities, were signed as a part of the onboarding process.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	Microsoft's Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage. Employees are required to acknowledge agreements to return Microsoft assets upon termination.	• Inspected a sample NDA to ascertain that the agreement included requirements for asset protection, and asset return upon termination of employment. • Obtained the total population of new hires from the HR system from the examination period. Selected a sample of new hires to ascertain that NDAs were signed at the time of onboarding. • Obtained and inspected the Reporting Concerns About Misconduct policy, to ascertain if policies around notification of incidents were documented.	
SOC2 - 14	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information, should be identified and regularly reviewed.	• Inquired of management regarding the process for requiring employees, contractors, and third-party users to follow established security policies and procedures. • Inquired of management on the process for identifying and reviewing requirements that were included in the confidentiality or non-disclosure agreements. • Identified the population of individuals that were new to the Microsoft Azure environment. • Obtained and inspected the security policy and procedure agreements signed by an employee, contractor, or third party for a sample of new users.	No exceptions noted.
SOC2 - 15	Azure has established baselines for OS deployments. Azure employs mechanisms to re-image production servers with the latest baseline configurations at least once a month or detect and troubleshoot exceptions or deviations from the baseline configuration in the production environment. The Azure OS and component teams review and update configuration settings and	• Inquired of management regarding the baseline process for Azure services, including scanning environments for baseline compatibility. • Obtained and inspected the baseline configurations to ascertain that baselines were established and reviewed on an annual basis. • For a sample of services, obtained a completed baseline scan from the period or log of monthly reimaging. Inspected scan results and obtained corresponding justifications for differences or documented resolutions.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	baseline configurations at least annually.		
SOC2 - 18	Relevant statutory, regulatory, and contractual requirements and the organization’s approach to meet these requirements for each information system and the organization, should be explicitly defined, documented, and kept up to date.	• Inquired of management regarding the procedures in place for identifying relevant statutory, regulatory, and contractual requirements, and making relevant updates to documentation or procedures accordingly. • Obtained and inspected calendar invite and the meeting minutes for the meetings between the Azure Global and Corporate, External, and Legal Affairs (CELA) teams to ascertain that they occurred on a regular basis. • Obtained and inspected policy, procedure, and agreement documents to ascertain that they included relevant and current statutory, regulatory, and contractual requirements.	No exceptions noted.
SOC2 - 19	A compliance program is managed with representation from various cross-functional teams and external parties to identify and manage compliance with relevant statutory, regulatory and contractual requirements.	• Inquired of management regarding the process in place for managing compliance with relevant statutory, regulatory and contractual requirements, with the involvement of various cross-functional teams including Corporate, External, and Legal Affairs (CELA), and Azure Global. • Obtained and inspected meeting invites and meeting minutes to ascertain that the meeting between Azure Global and various cross-functional teams such as CELA, and external parties such as government agencies, occurred on a regular basis. • Observed CELA communications regarding regulatory compliance to ascertain that it addressed relevant statutory, regulatory and contractual requirements.	No exceptions noted.
SOC2 - 20	Azure performs periodic Information Security Management System (ISMS) reviews and reviews results with management. This involves monitoring ongoing	• Inquired of management regarding the process for performing the Information Security Management System (ISMS) review. • Inquired of management regarding the process for planning and performing audit activities.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	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. Audit activities are planned and agreed upon in advance by stakeholders and any access required to perform the audits requires approval.	• Obtained and inspected the latest ISMS review to ascertain that the review was performed and results, including scope and applicability, were reviewed with management. • Obtained audit and compliance meeting invites, decks and newsletters to ascertain that audit activities were planned and reviewed with management prior to executing any audits.	
SOC2 - 25	Security risks related to external parties (such as customers, contractors, and vendors) are identified and addressed within the Azure environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Corporate, External, and Legal Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements.	• Inquired of management regarding the risk assessment process and how risks are identified and addressed related to external parties (such as customers, contractors and vendors). • Obtained and inspected the latest risk assessment performed by Microsoft Azure management to ascertain that it was complete. • Obtained and inspected the Statement of Work (SOW) template citing external parties' access was restricted authoritatively based on the risk assessment performed.	No exceptions noted.
SOC2 - 26	Microsoft Azure 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.	• Inquired of 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.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		• Obtained and inspected the risk assessment reports for the latest risk assessment performed by Microsoft Azure management for the identified risk domains, to ascertain that threats to security were identified and the risk from these threats was assessed.	
SOC2 - 27	Microsoft Azure undergoes independent audits and assessments, to monitor and verify compliance with security requirements, at least annually. Findings are recorded, reviewed, prioritized, and remediation plans are developed.	• Inquired of management regarding the various independent audits and assessments performed at least annually. • Obtained audit results and ascertained that findings were recorded, reviewed, prioritized, and remediation plans were developed.	No exceptions noted.
SOC2 - 28	Customer data is accessible within agreed upon services in data formats compatible with providing those services.	• Inquired of management regarding the accessibility of data from agreed upon services in data formats compatible with the services. • Selected a sample of services and obtained the published lists of data formats that the services support. • For a sample of data formats, observed the extraction of data and ascertained that customer data was accessible in the data formats.	No exceptions noted.
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.	• Inquired of 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.

Control ID	Control Activity	Test Procedures	Results of Tests
C5 - 2	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.	• Inquired of 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 - 3	The architecture of the Azure production network is documented as part of the inventory process. Metadata describing the network attributes (i.e. location, tier, and connections) are dynamically generated and updated as part of standard operations.	• Inquired of management regarding the procedures in place to document and update the architecture of the Azure production network. • Obtained and inspected network overview documentation including metadata and network inventory listings to ascertain that the architecture of the Azure production network was established, detailed the essential network attributes, and was updated as part of standard operations.	No exceptions noted.
C5 - 4	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	• Inquired of management to understand the procedures established to evaluate, review, notify and respond to government investigative demands for customer data. • Obtained and inspected the procedures established for government investigative demands for customer data and ascertained that they were reviewed on an annual basis.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	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.		
C5 - 5	Customer metadata is collected, retained, and removed based on the documented procedures.	• Inquired of management to understand the process regarding customer metadata collection, retention and deletion. • Inspected the metadata log retention configurations to ascertain that mechanisms existed for collecting, retaining and deleting customer metadata in accordance with documented procedures. • For a sample of test subscription, inspected evidence to ascertain that the process of collecting, retaining, and deleting customer metadata is in accordance with documented procedures.	No exceptions noted.
C5 - 6	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.	• Inquired of 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. • Inspected the security group configuration and ascertained that only authorized individuals were part of the security group that had access to the logging and monitoring infrastructure.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
C5 - 7	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.	• Inquired of management to understand the procedures in place for monitoring availability of the logging and monitoring infrastructure. • Through inspection, ascertained 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 - 8	Azure has established an Audit Log Management policy. Log and monitor access is restricted to only authorized staff with a business need to access such systems.	• Inquired of management regarding policies and procedures in place for audit log management, particularly pertaining to the collection, protection, and retention of these logs. • Obtained documented policies and procedures for audit log management within Microsoft Azure and inspected documentation and event immutability configurations to ascertain that procedures for collection, protection, and retention of audit logs were documented and enforced. • Obtained and inspected immutability configuration settings to ascertain that audit logs cannot be modified and segregation of duties is followed to disable immutability. • Obtained and inspected the configuration setting to ascertain that the logs are retained as per the documented procedures and deleted after the retention period is complete.	No exceptions noted.
C5 - 9	Microsoft Azure has established policies for mobile computing devices to meet appropriate security practices prior to being connected to the production environment.	• Inquired of management that a documented policy exists that specifies the rules and requirements applicable to mobile computing devices. • Obtained and inspected Azure's mobile computing policy to ascertain that it included applicable information security requirements.	No exceptions noted.
C5 - 10	Microsoft Azure components are configured to use Coordinated Universal Time (UTC) time and the	• Inquired of management regarding the procedures in place for time synchronization across the various Azure components. Additionally, inquired if Azure uses a centralized synchronized	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	clocks are synchronized with the domain controller server.	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 including configurations to sync time and clocks across the Azure components, including domain controllers, to UTC.	
C5 - 11	Azure has published a standard set of APIs with an ecosystem of tools and libraries on the Azure Portal.	• Inquired of management regarding the list of Application Programming Interfaces (APIs) that Azure offers to customers. • Inspected the policy and procedure to document the list of APIs and SDKs. Additionally, inspected Azure API reference webpage to ascertain that the list of APIs offered by Azure to customers were published in a centralized repository (webpage) and were as per the industry standards. • Inquired of management regarding the policy and procedures in place for services to document their list of Application Programming Interfaces (APIs) and SDKs that Azure offers to customers for interoperability and portability.	No exceptions noted.
C5 - 12	Azure has a shared responsibility model available on the trust center website describing the responsibilities between Azure and its customers.	• Inquired of management regarding the shared responsibility model between Azure and its customers. • Obtained the link and inspected the trust center website and ascertained that the shared responsibility model is available to customers. • Obtained and inspected the shared responsibility model self-assessment questionnaire filled by management to ascertain that shared responsibilities are defined for relevant controls / criteria.	No exceptions noted.
C5 - 13	Microsoft Capacity Management team projects future capacity requirements based on internal operational reports, revenue	• Inquired of management regarding the capacity planning process and capacity review model by management.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	forecasts and inputs from internal component teams.	• For the sampled months, obtained and inspected the monthly capacity planning review decks to ascertain that the necessary parameters were reviewed and considered.	
C5 - 14	Microsoft Azure has established forensic procedures to support potential legal action after an information security incident.	• Inquired of 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.
ELC - 1	Microsoft's values are accessible to employees via the Values SharePoint site and are updated as necessary by management.	• Inquired of 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 & 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 & 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.	• Inquired of management to ascertain that Standards of Business Conduct (SBC) is established and made available internally and externally. • 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.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
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.	• Inquired of management 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 on an annual basis, as listed in its calendar. 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.	• Inquired of management 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.
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.	• Inquired of 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 directs the services of the Internal Audit. • Obtained and inspected the Internal Audit plan and ascertained that the assurance activities are 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	• Inquired of management regarding the process for:	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	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.	– 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.	
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.	• Inquired of management 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). • For a sample of employees, obtained evidence of occurrence of periodic connects to ascertain that the connects occurred at least annually.	No exceptions noted.
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.	• Inquired of management 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	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		Committee's responsibility included reviewing the succession plan for CEO and other executive officers, on an annual basis.	
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.	• Inquired of management 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 5:
Other Information Provided by Management of Microsoft

Section 5: Other Information Provided by Management of Microsoft

The following information is provided for informational purposes only and has not been subjected to the procedures applied in the examination. Accordingly, Deloitte & Touche LLP expresses no opinion on the following information.

Azure Compliance

Microsoft Azure supports compliance with a broad set of industry-specific laws and meets broad international standards. Azure has ISO 27001, ISO 27017, ISO 27018, ISO 22301, and ISO 9001 certifications, PCI DSS Level 1 validation, SOC 1 Type 2 and SOC 2 Type 2 attestations, HIPAA Business Associate Agreement, and HITRUST certification. Operated and maintained globally, Microsoft Azure 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 Azure Compliance site.

Infrastructure Redundancy and Data Durability

Azure mitigates the risk of outages due to failures of individual devices, such as hard drives or even entire servers through the following:

- Data durability of Azure Storage (Blobs (including Azure Data Lake Storage Gen2), Disks, Files, Queues, Tables) including Cool and Premium, facilitated by maintaining redundant copies of data on different drives located across fully independent physical storage subsystems. Copies of data are continually scanned to detect and repair bit rot.
- Cloud Services availability, maintained by deploying roles on isolated groupings of hardware and network devices known as fault domains. The health of each compute instance is continually monitored and roles are automatically relocated to new fault domains in the event of a failure.
- Network load balancing, automatic OS and service patching is built into Azure. The Azure application deployment model also upgrades customer applications without downtime by using upgrade domains, a concept similar to fault domains, which helps ascertain that only a portion of the service is updated at a time.

Data Backup and Recovery

In addition to the core data durability built into Azure, Azure provides customers with a feature to capture and store point-in-time backups of their stored Azure data. This allows customers to protect their applications from an event of corruption or unwanted modification or deletion of its data.

Microsoft Azure E.U. Data Protection Directive

Microsoft offers contractual commitments for the safeguarding of customer data as part of the Product Terms, Microsoft Licensing Terms and Documentation.

- A Data Processing Agreement that details our compliance with the E.U. Data Protection Directive and related security requirements for Azure core features within ISO / IEC 27001:2013 scope.
- E.U. Model Contractual Clauses that provide additional contractual guarantees around transfers of personal data for Azure core features within ISO / IEC 27001:2013 scope.

Additional Resources

The following resources are available to provide more general information about Azure and related Microsoft services:

- Microsoft Azure Home - General information and links to further resources about Azure: http://azure.microsoft.com
- Microsoft Trust Center includes details regarding Compliance, Service Agreement and Use Rights, Privacy Statement, Security Overview, Service Level Agreements, and Legal Information http://www.microsoft.com/en-us/trustcenter
- Azure Documentation Center - Main repository for developer guidance and information: https://azure.microsoft.com/en-us/documentation
- Microsoft's Security Development Lifecycle - SDL is Microsoft's security assurance process that is employed during the development of Azure: https://www.microsoft.com/en-us/securityengineering/sdl/
- Microsoft's Global Datacenters is the group accountable for delivering a trustworthy, available online operations environment that underlies Microsoft Azure: https://azure.microsoft.com/en-us/global-infrastructure/
- Microsoft Security Response Center - Microsoft security vulnerabilities, including issues with Azure, can be reported to: https://www.microsoft.com/en-us/msrc or via email to secure@microsoft.com
- Azure OpenAI - Learn more about Azure OpenAI Data, Privacy, and Security Data, privacy, and security for Azure OpenAI Service - Azure AI services

Management's Response to Exceptions Noted

The table below contains Management's response to the exceptions identified in section 4 - 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 above.

Control ID	Control Activity	Exception Noted	Management Response
DS - 1	Cryptographic certificates, keys, and customer access keys used for communication between Azure services and other internal components are stored securely and are rotated on a periodic basis.	Three of 24 sampled secrets tested during the period 4/1/2024 to 12/31/2024 were not rotated as per the secret rotation cadence defined in the documented procedures. Further, tested 11 sampled secrets subsequent to December 31, 2024, and no additional exceptions were noted. Additionally, certain internal Microsoft platform keys were not rotated according to the prescribed cadence outlined in the internal policy. As mitigation, these keys were	Sampled Secrets For the one sampled secret detected during the September 30, 2024 report; the secret that was owned by Azure Data Manager for Energy has since been rotated. Furthermore, Azure Data Manager for Energy has implemented additional monitoring procedures to help prevent delays in rotating secrets per internal policy and a fix to auto rotate this secret going forward. For the two sampled secrets detected during the June 30, 2024 report; these secrets were owned by Azure VMWare and Azure Monitor and the secrets were access keys for storage accounts previously utilized by internal partner service teams that did not store customer data and have since been deleted. Management confirmed access to all keys was controlled through Just-in-Time (JIT) temporary access and securely stored using Azure Key Vault encryption.

Control ID	Control Activity	Exception Noted	Management Response
		protected through other security practices, including additional encryption. Separately, as part of its investigation into the actions of Midnight Blizzard, Microsoft identified passwords and secrets impacting certain in-scope Azure services that were accessed by the threat actors through code repositories or Microsoft corporate email. Furthermore, Internal Audit of Microsoft identified multiple secrets associated with four in-scope services that were not rotated during the past year.	There have been no additional failures for this finding since it was first identified in the September 30, 2024 SOC reports. Platform Keys Through internal processes, Microsoft identified that certain internal platform keys were excluded from the rotation policy cadence and shared this information with our external auditors. As a mitigation, these platform keys are protected through key wrapping using AES 256 encryption and rotation for the wrapping keys occur within a schedule compliant with internal policies. Access to the internal platform keys is managed through the Just-in-Time (JIT) temporary access service requiring explicit approval from senior leadership. Only senior members of the engineering team can approve JIT requests for platform keys. Additionally, access to approve all JIT requests are included in quarterly access reviews. There have been no additional failures related to this finding since it was first identified in the 3/31/2024 SOC reports. Cyber Incident Based on our internal investigation regarding the Midnight Blizzard incident, impacted passwords and secrets belonging to in-scope Azure services have been rotated or remediated. There are robust and effective controls included in this report related to authentication, operator access, encryption, and monitoring and detection designed to prevent or detect attempts by the threat actors to make unauthorized modifications to our in-scope offerings. There has been no evidence indicating the threat actor made unauthorized changes to the offerings covered within this report. Microsoft has launched the Secure Future Initiative to further prepare for the increasing scale of cyberattacks. There have been no additional failures related to this finding since it was first identified in the March 31, 2024 SOC reports. Microsoft has determined that the incident was closed on October 15, 2024. Internal Audit Microsoft Internal Audit identified that certain production keys used by four in-

Control ID	Control Activity	Exception Noted	Management Response
			scope services have not been rotated per internal policy. Of the four services reviewed, two fell within the current reporting period (April 1, 2024–March 31, 2025), while the other two occurred in the prior reporting period (January 1, 2024–December 31, 2024). The two services that fell within the current reporting period are part of Azure AI Foundry Portal, Azure Open Datasets, Azure OpenAI Service, Azure Machine Learning, and Microsoft Entra ID offerings. These keys have been rotated or are actively being deleted as a result of this finding. Although the keys were not rotated per internal policy, the impacted Azure offerings manage access to the keys through Just-in Time (JIT) and are stored in secure secret repositories.
SDL - 1	Development of new features and changes to the Azure services follow a defined approach based on the Microsoft Security Development Lifecycle (SDL) methodology. The SDL review for each service is performed on an annual basis.	For 15 of the 36 sampled services, SDL review was not completed within the annual cadence. For the period 04/01/2024 to 08/31/2024, Internal Audit of Microsoft identified one additional sample that did not meet the annual SDL review cadence. Additionally, Internal Audit of Microsoft identified one sampled service in which two exceptions were not approved timely and by the appropriate personnel as per Microsoft's SDL Methodology.	Sampled Services The Security Development Lifecycle (SDL) process includes both an annual attestation and continuous automated monitoring to ensure compliance with SDL requirements. Although the annual attestation for the 16 services was completed after the internal service level agreement deadline, management has confirmed that SDL requirements were consistently met throughout the audit period. This has been verified by the automated internal monitoring system. Additionally, Internal Audit discovered during their testing a sampled service did not follow the proper process for submitting an exception request. Subsequent to this finding, the exception request was submitted through the correct process and approved by the appropriate personnel. To help prevent future occurrences, the process has been enhanced to automatically facilitate following the correct process. Out of the aforementioned 17 services, six were identified in the current testing period while the other 11 were identified in prior testing periods. The six services that pertain to the current reporting period are part of the Dataverse, Microsoft Entra ID, Azure Container Apps, Azure Cosmos DB, Azure

Control ID	Control Activity	Exception Noted	Management Response
			Health Data Services, and Microsoft Entra Domain Services offerings. Compliance with SDL requirements is reinforced by various Data Security, Vulnerability Management, and Operator Access controls, which have been tested and found to operate effectively. To strengthen compliance with internal policies, management has engaged executive leadership to re-emphasize the importance of timely completion of annual assessments.
CM - 2	Secondary approval is required prior to all pull request check-ins to the production build, enforcing segregation among designated personal when implementing changes.	Management self-identified a vulnerability that could have allowed a single individual to submit and approve code bypassing SOD controls at the pull request level by using two user accounts owned by the same individual (i.e. Corp and Alt accounts). Management identified and disclosed 31 related instances from a large quantity of pull requests where developers self-approved their pull requests before checking them into the production build, leveraging multiple user accounts that they owned. Additionally, tested 15 change samples subsequent to September 30, 2024 and no additional exceptions were noted.	Following the identification of Segregation of Duties (SOD) violations, management conducted a comprehensive analysis covering 100% of all in-scope pull requests. This analysis revealed 31 instances where individuals self-approved changes to be merged into a production build. For the 31 instances, the changes were pre planned and had received the necessary approvals prior to deployment which includes additional segregation of duties validation as part of the CM-3 control. As a result of this finding, automated monitoring and alerting has been implemented to detect future instances of self-approval for pull requests. There have been no additional failures for this control since it was first identified in the September 30, 2024 SOC reports.
CM - 12	Azure has implemented tools to perform integrity verification checks to detect unauthorized changes to software, firmware and information.	For the period April 1, 2024 to March 31, 2025, Internal Audit Team of Microsoft noted that code-signing was not configured for seven of the build pipelines associated with five of the in-scope services.	Four of the five in-scope services with release pipelines lacking code signing fell within the current reporting period (April 1, 2024 - March 31, 2025), while the remaining service was from the prior reporting period (January 1, 2024 - December 31, 2024). The services identified in the current period are part of the Azure AI Foundry Portal, Azure Open Datasets, Azure OpenAI Service, and Azure Machine Learning offerings. Although code signing was not enabled, all other change management controls were met. To

Control ID	Control Activity	Exception Noted	Management Response
		No additional exceptions were noted in our independent testing.	address this gap, all affected offerings have committed to re-enabling code signing.
DS - 8	Data Protection Services (DPS) backs up data for properties based on a defined schedule and upon request of the properties. Data is retained according to the data type identified by the property. DPS investigates backup errors and skipped files and follows up appropriately	Management identified a vulnerability in the supporting third-party software used in scheduling of their internal offline backups. As a result, management paused backups, resulting in the control not operating effectively from February 22, 2025.	Microsoft conducts ongoing global security research and threat hunting. Upon identifying a vulnerability in third-party software used for offline data backups, leadership made the decision to pause those operations. Azure continues to provide online backups through geo-redundant replication in alignment with DS-5 and DS-6 controls. Business continuity controls, specifically BC-1, BC-4, and BC-9, covering services and data centers are reviewed and tested annually, and have proven effective in supporting successful failover during service disruptions.
DS - 9	Backup restoration procedures are defined and backup data integrity checks are performed through standard restoration activities.	Management identified a vulnerability in the supporting third-party software used in scheduling of their internal offline backups. As a result, management paused backups, resulting in the control not operating effectively from February 22, 2025.	Microsoft conducts ongoing global security research and threat hunting. Upon identifying a vulnerability in third-party software used for offline data backups, leadership made the decision to pause those operations. Azure continues to provide online backups through geo-redundant replication in alignment with DS-5 and DS-6 controls. Business continuity controls, specifically BC-1, BC-4, and BC-9, covering services and data centers are reviewed and tested annually, and have proven effective in supporting successful failover during service disruptions.
DS - 11	Data corresponding to Azure is backed up to another region other than the primary data location and retained as per the retention policy.	Management identified a vulnerability in the supporting third-party software used in scheduling of their internal offline backups. As a result, management paused backups, resulting in the control not operating effectively from February 22, 2025.	Microsoft conducts ongoing global security research and threat hunting. Upon identifying a vulnerability in third-party software used for offline data backups, leadership made the decision to pause those operations. Azure continues to provide online backups through geo-redundant replication in alignment with DS-5 and DS-6 controls. Business continuity controls, specifically BC-1, BC-4, and BC-9, covering services and data centers are reviewed and tested annually, and have proven effective in supporting successful failover during service disruptions.
VM - 6	Procedures to monitor the Azure platform components for known security vulnerabilities have	Internal Audit of Microsoft identified multiple vulnerabilities associated with five in-scope services that were not remediated	The services relevant for this issue are part of the Azure AI Foundry Portal, Azure Open Datasets, Azure OpenAI Service, and Azure Machine Learning offerings. Although some assets were identified to have untimely

Control ID	Control Activity	Exception Noted	Management Response
	been established. Identified security vulnerabilities are remediated.	in a timely manner within the expected SLA. No additional exceptions were noted in our independent testing.	resolution to known vulnerabilities, several effective mitigating controls—such as endpoint encryption, network segmentation, packet filtering, and Security Information and Event Management (SIEM) were actively in place and effective throughout the period.
PE - 4	Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.	For 1 of 17 sampled datacenters, while there are various layers of physical access mechanisms that were determined to be properly implemented, two instances of physical access mechanisms were not properly administered: - A trash door that provides access to the loading area was not fully closed. - While keycards were required to enter the generator area, several generator enclosures within the area that are normally secured with temporary-use physical keys had broken or unsecured locks.	The physical access mechanism relates to a trash door that was not fully closed. This door only provides access to the loading area of the data center. Additionally, a secured gate requiring prior authorization controls entry into the data center perimeter, including the trash area. Since the door does not lead into the data center itself and access to the perimeter is restricted, management considers this finding to pose no risk. The second physical access mechanism pertains to the individual generator doors not being locked inside the generator area. Access to the generator area requires multiple layers of authorization to access and is governed by role-based access controls and subject to quarterly reviews. Once inside, personnel are considered appropriate to access the individual generator doors and internal policy does not require these sub-areas in the enclosure to be locked. Since access to the area is strictly controlled and there is no violation of internal policy, management considers this finding to pose no risk.
PE - 5	The datacenter facility is monitored 24x7 by security personnel.	For 1 of the 32 sampled cameras, the tapes were not retained in accordance with the documented operating procedures.	The sampled camera experienced a hardware issue that prevented tape retention that has since been resolved; however, it did not affect the live CCTV feed or management's ability to conduct 24/7 monitoring of the facility. Management obtained evidence of security patrol logs, footage from other facility cameras, and footage of the monitoring room - demonstrating that live monitoring remained effective.

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 criteria. User entities and other interested parties should determine whether the user entities have established sufficient controls in these areas:

- Customers are responsible for managing compliance with applicable laws / regulations.
- Customers are responsible for establishing appropriate controls over the use of their Microsoft Accounts and passwords.
- Customers are responsible for disabling / deleting account access to their Azure services upon employee and contractor role change or terminations.
- Customers are responsible for implementing workstation timeout for extended periods of inactivity.
- Customers are responsible for reviewing the access activities associated with their accounts and their VM applications.
- Customers are responsible for protecting the credentials associated with their deployment profiles.
- Customers are responsible for following appropriate security practices during development and deployment of their applications on Azure Web Apps.
- Customers are responsible for configuring their Web Apps deployments to log appropriate diagnostic information and monitoring for security related events.
- Customers are responsible for specifying strong credentials used with service identities and management service accounts and managing them for continued appropriateness.
- Customers are responsible for ensuring the supervision, management and control for access to key systems.
- Customers are responsible for verifying the security of patching, and maintaining any third party applications and / or components that they install on their production environment.
- Customers' administrators are responsible for the selection and use of their passwords.
- Customer entities are responsible for notifying the MFA service of changes made to technical or administrative contact information.
- Customers are responsible for maintaining their own system(s) of record.
- Customers are responsible for ensuring the supervision, management and control of the use of MFA services by their personnel.
- Customers are responsible for developing their own Disaster Recovery and Business Continuity Plans that address the inability to access or utilize MFA services.
- Customers are responsible for ensuring the confidentiality of any user IDs and passwords used to access MFA systems.
- Customers are responsible for ensuring that user IDs and passwords are assigned to authorized individuals.
- Customers are responsible for ensuring that the data submitted to the MFA service is complete, accurate and timely.
- Customers are responsible for immediately notifying the MFA service of any actual or suspected information security breaches, including compromised user accounts.
- Customers are responsible for determining, implementing and managing encryption requirements for their data within the Azure platform where Azure does not enable it by default and / or can be controlled by the customer.
- Customers are responsible for securing certificates used to access Azure SMAPI.
- Customers are responsible for selection of the access mechanism (i.e., public or signed access) for their data.
- Customers are responsible for determining the configurations to be enabled on their VMs.
- Customers are responsible for backup of their data from Azure to local storage upon Azure subscription termination.

- Customers are responsible for appropriate protection of the secrets associated with their accounts.
- Customers are responsible for designing and implementing interconnectivity between their Azure and on-premises resources.
- Customers are responsible for specifying authorization requirements for their Internet-facing messaging end points.
- Customers are responsible for encrypting content using the SDK provided by Media Services.
- Customers are responsible for the rotation of DRM and content keys.
- Customers are responsible for following a Secure Development Lifecycle methodology for their applications developed on Azure.
- Customers are responsible for application quality assurance prior to promoting to the Azure production environment.
- Customers are responsible for monitoring the security of their applications developed on Azure.
- Customers are responsible for reviewing public Azure security and patch updates.
- Customers not signed up for auto-upgrade are responsible for applying patches.
- Customers are responsible for reporting to Microsoft the incidents and alerts that are specific to their systems and Azure.
- Customers are responsible to support timely incident responses with the Azure team.
- Customers are responsible for designing and implementing redundant systems for hot-failover capability.
- Customers are responsible to assign unique IDs and secured passwords to users and customers accessing their instance of the API Management service.
- Customers are responsible to secure their API using mutual certificates, VPN or the Azure ExpressRoute service.
- Customers are responsible for using encrypted variable asset to store secrets while utilizing the Automation service.
- Customers are responsible for reviewing the access activities associated with their Intune enrolled devices.
- Customers are responsible for determining and implementing encryption requirements for their Intune enrolled devices and on-premises resources.
- Customers are responsible for securing certificates used to access Intune (iOS Onboarding certificate, Windows Phone Code Signing Certificates for Windows Phone, any certificate used to sign Enterprise Windows Applications, and Certificate Registration Point (CRP) Signing certificates used in VPN / WiFi Profiles).
- Customers are responsible for determining the applications and policies to be deployed to their Intune enrolled devices.
- Customers are responsible for designing and implementing interconnectivity between their Intune subscription and on-premises resources (specifically any VPN infrastructure, System Center Configuration Manager infrastructure, and the Exchange Connector).
- Customers utilizing the Azure ExpressRoute service are responsible for ensuring their on-premises infrastructure is physically connected to their connectivity service provider infrastructure.
- Customers are responsible for ensuring the service with their connectivity provider is compatible with the Azure ExpressRoute service.
- Customers are responsible for ensuring that their connectivity provider extends connectivity in a highly available manner so that there are no single points of failure.

- Customers utilizing the Azure ExpressRoute service are responsible to set up redundant routing between Microsoft and the customer’s network to enable peering.
- Customers co-located with an exchange or connecting to Microsoft through a point-to-point Ethernet provider are responsible to configure redundant Border Gateway Protocol (BGP) sessions per peering to meet availability SLA requirements for Azure ExpressRoute.
- Customers are responsible for appropriate setup and management of Network Address Translation (NAT) to connect to Azure services using Azure ExpressRoute.
- Customers are responsible for ensuring the NAT IP pool advertised to Microsoft is not advertised to the Internet when utilizing the Azure ExpressRoute service.
- Customers are responsible for adhering to peering requirements with other Microsoft Online Services such as Microsoft 365 when utilizing the Azure ExpressRoute service.
- Customers utilizing the Azure ExpressRoute service are responsible for encrypting their data while in transit.
- Customers utilizing the Azure ExpressRoute service are responsible for protection of their Cloud Services and resource groups through use of appropriate security and firewalling.
- Customers are responsible for implementing appropriate authentication mechanisms and only granting admin access to appropriate individuals to maintain the integrity of their Microsoft Entra ID tenant.
- Customers utilizing Microsoft Entra ID services are responsible for implementing appropriate authentication mechanisms and limiting admin access to appropriate individuals to maintain integrity of their SaaS applications.
- Customers are responsible to implement logical access controls to provide reasonable assurance that unauthorized access to key systems will be restricted.
- Customers are responsible for backing up keys that they add to Azure Key Vault.
- Customers are responsible for appropriately testing application systems deployed in the Dynamics 365 environment prior to deployment in the production environment.
- Customers are responsible for appropriately testing and approving customer developed customizations and extensions prior to deployment in the Dynamics 365 production environment.
- Customers are responsible for understanding and adhering to the contents of their service contracts, including commitments related to system security, availability, processing integrity, and confidentiality.
- Customers are responsible for managing their inputs and data uploads to Dynamics 365 for completeness, accuracy, and timeliness to meet commitments related to system security, availability, processing integrity, and confidentiality.
- Customers are responsible for notifying Microsoft of any unauthorized use of Dynamics 365 accounts.
- Customers are responsible for the authorization of transactions processed in the Dynamics 365 system.
- Customers are responsible for validating the completeness and accuracy of customized reporting in the Dynamics 365 environment.
- Customers are responsible for hardening virtual machine images as per their requirements.
- Customers are responsible for responding to data subject requests for customer data or system generated logs.
- Customers are responsible for the management of any on-premises components for in-scope offerings and services.