Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

To: Microsoft Azure and Dynamics 365 Services customers

Microsoft recognizes the need to maintain an appropriate internal control environment and report on the effectiveness of, as well as material changes to, its system of internal control. This letter is to clarify that the Microsoft Dynamics 365 organization was consolidated into the Microsoft Azure organization in mid-2018. As a result, the compliance teams have worked to consolidate the Microsoft Dynamics 365 and Dynamics 365 for Government SOC controls into the Microsoft Corporation - Azure Including Dynamics 365 SOC 2 Type 2 report, beginning with the 9/30/2019 period end report. The scope of Microsoft Dynamics 365 and Dynamics 365 for Government SOC controls, services, offerings and audit period are fully covered in the Microsoft Corporation - Azure Including Dynamics 365 SOC 2 Type 2 report. "Azure", when referenced in this report, comprises "Microsoft Azure", "Microsoft Dynamics 365", "Online Services", and the supporting datacenters listed in this report. Refer to "Azure and Azure Government Report Scope Boundary" in Section III of the report to find a listing of Dynamics 365 offerings covered in the report.

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 Azure 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 Corporation - Azure Including Dynamics 365

(Azure & Azure Government)

System and Organization Controls (SOC) 2 Report

April 1, 2019 - March 31, 2020

Table of contents

Executive Summary

	Microsoft Azure	
Scope	Microsoft Azure, Microsoft Dynamics 365 and Microsoft Datacenters	
Period of Examination	April 1, 2019 to March 31, 2020	
Applicable Trust Services Criteria	Security, Availability, Processing Integrity, and Confidentiality	
Datacenter Location(s)	• Abu Dhabi (AUH20) • Ambattur, India (MAA01) • Amsterdam, Netherlands (AM1/2/3, AMS04/05/06/07/20/21/23) • Ashburn, VA (BL2/3/5/6/7/21/22/23/30) • Berlin, Germany (BER20) • Boydton, VA (BN1/3/4/6/7/8/14) • Bristow, VA (BLU) • Busan, South Korea (PUS01/20) • Campinas, Brazil (CPQ01/02/20) • Canberra, Australia (CBR20/21) • Cape Town, South Africa (CPT20) • Cardiff, United Kingdom (CWL20) • Cheyenne, WY (CYS01/04/05) • Chicago, IL (CH1/3/4, CHI20/21) • Cyberjaya, Malaysia (KUL01) • Des Moines, IA (DM1/2/3, DSM05/06/08) • Dighi, India (PNQ01) • Dubai (DXP20) • Dublin, Ireland (DB3/4/5, DUB06/07/08/11/20/21/24/31) • Durham, United Kingdom (MME20) • Fortaleza, Brazil (FOR01) • Frankfurt, Germany (FRA21) • Geneva, Switzerland (GVA20) • Hong Kong (HK1/2, HKG20/21) • Johannesburg, South Africa (JNB20/21/22) • London, United Kingdom (LON20/21/22/23/24) • Luxembourg A: SecureIT (LUA) • Macquarie Park, Australia (SYD03)	• Manassas, VA (MNZ20) • Marseille, France (MRS20) • Melbourne, Australia (MEL01/20/21) • Mumbai, India (BOM01) • Osaka, Japan (OSA01/02/20/21/22) • Oslo, Norway (OSL20) • Paris, France (PAR20/21/22/23) • Phoenix, AZ (PHX20/21) • Quebec, Canada (YQB20) • Quincy, WA (CO1/2, MWH01/02/03) • Reston, VA (BL4/31) • Rio de Janeiro, Brazil (RIO01) • San Antonio, TX (SN1/2/3/4/5/6, SAT09) • San Jose, CA (SJC31) • Santa Clara, CA (BY1/2/3/4/5/21/22/24/30) • Santiago, Chile (SCL01) • Sao Paulo, Brazil (GRU) • Seoul, South Korea (SEL20/21) • Singapore (SG1/2/3, SIN20) • Stavanger, Norway (SVG20) • Sterling, VA (BL20) • Sydney, Australia (SYD21/22/23/25) • Tokyo, Japan (KAW, TYO01/20/21/22/31) • Toronto, Canada (YTO20/21) • Vantaa, Finland (HEL01) • Vienna, Austria (VIE) • Zurich, Switzerland (ZRH20)

Microsoft Azure		
Edge Sites	• Ashburn, VA (ASH) • Athens, Greece (ATH01) • Atlanta, GA (ATA) • Auckland, New Zealand (AKL01) • Bangkok, Thailand (BKK30) • Barcelona, Spain (BCN30) • Berlin, Germany (BER30) • Boston, MA (BOS01) • Brisbane, Australia (BNE01) • Brussels, Belgium (BRU30) • Bucharest, Romania (BUH01) • Budapest, Hungary (BUD01) • Busan, South Korea (PUS03) • Cape Town, South Africa (CPT02) • Chicago, IL (CHG) • Copenhagen, Denmark (CPH30) • Dallas, TX (DAL) • Denver, CO (DEN02) • Dubai, United Arab Emirates (DXB30) • Frankfurt, Germany (FRA) • Geneva, Switzerland (GVA30) • Helsinki, Finland (HEL03) • Hong Kong (HKB) • Honolulu, HI (HNL01) • Houston, TX (HOU01) • Hyderabad, India (HYD30) • Jakarta, Indonesia (JKT30) • Johannesburg, South Africa (JNB02) • Kuala Lumpur, Malaysia (KUL30) • Lagos, Nigeria (LOS30) • Las Vegas, NV (LAS01) • Lisbon, Portugal (LIS01) • Los Angeles, CA (LAX) • Madrid, Spain (MAD30) • Manchester, United Kingdom (MAN30)	• Manila, Philippines (MNL30) • Marseille, France (MRS01) • Queretaro, Mexico (MEX30) • Miami, FL (MIA) • Milan, Italy (MIL30) • Montreal, Canada (YMQ01) • Mumbai, India (BOM02) • Munich, Germany (MUC30) • Nairobi, Kenya (NBO30) • New Delhi, India (DEL01) • Newark, NJ (EWR30) • New York City, NY (NYC) • Osaka, Japan (OSA31) • Oslo, Norway (OSL30) • Palo Alto, CA (PAO) • Paris, France (PAR02/PRA) • Perth, Australia (PER01) • Phoenix, AZ (PHX01) • Portland, OR (PDX31) • Prague, Czech Republic (PRG01) • San Jose, CA (SJC) • Santiago, Chile (SCL30) • Sao Paulo, Brazil (SAO03) • Seattle, WA (WST) • Seoul, South Korea (SLA) • Sofia, Bulgaria (SOF01) • Stockholm, Sweden (STO) • Taipei, Taiwan (TPE30/31) • Tokyo, Japan (TYA/TYB) • Toronto, Canada (YTO01) • Vancouver, Canada (YVR01) • Warsaw, Poland (WAW01) • Zagreb, Croatia (ZAG30) • Zurich, Switzerland (ZRH)
Subservice Providers	N/A	
Opinion Result	Unqualified	
Testing Exceptions	2	

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

Deloitte & Touche LLP
925 Fourth Avenue
Suite 3300
Seattle, WA 98104-1126
USA

Tel: 206-716-7000
Fax: 206-965-7000
www.deloitte.com

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

Microsoft Corporation
One Microsoft Way
Redmond, WA, 98052-6399

Scope

We have examined the attached description of the system of Microsoft Corporation (the "Service Organization" or "Microsoft") related to in-scope services and offerings for Microsoft Azure, Microsoft Dynamics 365, and Microsoft datacenters ("Azure") for Azure and Azure Government cloud environments[1] throughout the period April 1, 2019 to March 31, 2020 (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* ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the Description throughout the period April 1, 2019 to March 31, 2020 to provide reasonable assurance that Microsoft's 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")[2] set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.* We have also examined the suitability of the design and operating effectiveness of controls to meet the criteria set forth in the Cloud Security Alliance's (CSA) Cloud Controls Matrix (CCM) Version 3.0.1 control specifications ("CCM criteria") and the objectives set forth in the Bundesamt für Sicherheit in der Informationstechnik (BSI) Cloud Computing Compliance Controls 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 the cover letter on Microsoft's letterhead and the information included in Section V, "Supplemental Information Provided by Microsoft" is presented by management of Microsoft to provide additional information and is not a part of the Description. Information included in the cover letter and the information in Section V describing Service Organization's Compliance, Infrastructure Redundancy and Data Durability, Data Backup and Recovery, E.U. Data Protection Directive, Additional Resources, Management's

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

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

Response to Exceptions Noted, Dynamics Controls to Azure Controls Mapping, and User Entity Responsibilities, have not been subjected to the procedures applied in the examination of the Description and the suitability of the design and operating effectiveness of the controls, to achieve (a) Microsoft's service commitments and system requirements based on the applicable trust services criteria; (b) the CCM criteria; and (c) the objectives set forth in C5.

Service Organization's Responsibilities

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 were achieved. Microsoft has provided the accompanying assertion titled "Management's Assertion" about the Description and the suitability of design and operating effectiveness of controls stated therein. 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 (a) the Service Organization's service commitments and system requirements; (b) the CCM criteria; and (c) the objectives set forth in C5.

Service Auditors' 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. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the Description is presented in accordance with the description criteria, and the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that (a) the Service Organization's service commitments and system requirements were achieved based on the applicable trust services criteria; (b) the CCM criteria were achieved; and (c) the objectives set forth in C5 were achieved. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Obtaining an understanding of the system and the Service Organization's service commitments and system requirements.
- Assessing the risks that the Description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the Description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the Description were suitably designed to provide reasonable assurance that (a) the Service Organization achieved its service commitments and system requirements based on the applicable trust services criteria; (b) the CCM criteria were achieved; and (c) the objectives set forth in C5 were achieved.
- Testing the operating effectiveness of those controls stated in the Description to provide reasonable assurance that (a) the Service Organization achieved its service commitments and system requirements based on the applicable trust services criteria; (b) the CCM criteria were achieved; and (c) 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 Auditors' Independence and Quality Control

We have complied with the independence and other ethical requirements of the *Code of Professional Conduct* established by the AICPA. We applied the statements on quality control standards established by the AICPA 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 may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs. There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that (a) the Service Organization's service commitments and system requirements are achieved based on the applicable trust services criteria; (b) the CCM criteria are achieved; and (c) 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 tested, and the nature, timing, and results of our tests are listed in Section IV of the report.

Opinion

In our opinion, in all material respects,

a. The Description presents the system related to Microsoft's in-scope services and offerings, for Azure and Azure Government cloud environments, that was designed and implemented throughout the period April 1, 2019 to March 31, 2020, in accordance with the description criteria.

b. The controls stated in the Description were suitably designed throughout the period April 1, 2019 to March 31, 2020, to provide reasonable assurance that (a) Microsoft's service commitments and systems requirements would be achieved based on the applicable trust services criteria; (b) the CCM criteria would be achieved; and (c) the objectives set forth in C5 would be achieved, if the controls operated effectively throughout that period.

c. The controls stated in the Description operated effectively throughout the period April 1, 2019 to March 31, 2020, to provide reasonable assurance that (a) Microsoft's service commitments and system requirements were achieved based on the applicable trust services criteria; (b) the CCM criteria were achieved; and (c) the objectives set forth in C5 were achieved.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of Microsoft, user entities of the in-scope services and offerings, for Azure and Azure Government cloud environments system of Microsoft during some or all of the period April 1, 2019 to March 31, 2020, 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, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the Service Organization.

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

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

Deloitte & Touche LLP

April 30, 2020

Section II:
Management's Assertion

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

Section II: Management's Assertion

Microsoft Azure's Management Assertion

We have prepared the description of the system in Section III of Microsoft Corporation (the "Service Organization" or "Microsoft") throughout the period April 1, 2019 to March 31, 2020[3] (the "period") related to in-scope services and offerings for Microsoft Azure, Microsoft Dynamics 365, and Microsoft datacenters ("Azure") for Azure and Azure Government cloud environments (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* ("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, 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")[4] set forth in TSP Section 100, 2017 *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*; (b) the criteria set forth in the Cloud Security Alliance's (CSA) Cloud Controls Matrix (CCM) Version 3.0.1 control specifications ("CCM criteria") were achieved; and (c) the control objectives set forth in the Bundesamt für Sicherheit in der Informationstechnik (BSI) Cloud Computing Compliance Controls 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, 2019 to March 31, 2020 in accordance with the description criteria.

b. The controls stated in the Description were suitably designed throughout the period April 1, 2019 to March 31, 2020, to provide reasonable assurance that (a) Microsoft's service commitments and system requirements would be achieved based on the applicable trust services criteria; (b) the CCM criteria would be achieved; and (c) the objectives set forth in C5 would be achieved, if its controls operated effectively throughout that period.

c. The controls stated in the Description operated effectively throughout the period April 1, 2019 to March 31, 2020, to provide reasonable assurance that (a) Microsoft's service commitments and system requirements were achieved based on the applicable trust services criteria; (b) the CCM criteria were achieved; and (c) the objectives set forth in C5 were achieved.

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

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

Section III:
Description of Microsoft Azure System

Section III: Description of Microsoft 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 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
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

Trust Services Criteria	Description	Applicability Considerations
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 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 Boundary

Azure is global multi-tenant cloud platform that provides a public cloud deployment model. Azure Government is a US Government Community Cloud (GCC) 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[5]			
		Azure	Azure Government	Q4 FY19	Q1 FY20	Q2 FY20	Q3 FY20
Microsoft Datacenters							
Microsoft Datacenter and Operations Service		✓	✓	✓	✓	✓	✓

[5] Examination period scope Q4 FY19 extends from April 1, 2019 to June 30, 2019.
Examination period scope Q1 FY20 extends from July 1, 2019 to September 30, 2019.
Examination period scope Q2 FY20 extends from October 1, 2019 to December 31, 2019.
Examination period scope Q3 FY20 extends from January 1, 2020 to March 31, 2020.

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[5]			
		Azure	Azure Government	Q4 FY19	Q1 FY20	Q2 FY20	Q3 FY20
			Azure				
Compute	App Service	✓	✓	✓	✓	✓	✓
	Azure Functions	✓	✓	✓	✓	✓	✓
	Azure Service Fabric	✓	✓	✓	✓	✓	✓
	Batch	✓	✓	✓	✓	✓	✓
	Cloud Services[6]	✓	✓	✓	✓	✓	✓
	Virtual Machines	✓	✓	✓	✓	✓	✓
	Virtual Machine Scale Sets	✓	✓	✓	✓	✓	✓
Containers	Azure Container Service[7]	✓	✓	✓	✓	✓	✓
	Azure Kubernetes Service (AKS)[7]	✓	✓	✓	✓	✓	✓
	Azure Red Hat OpenShift (ARO)	✓	-	-	-	✓	✓
	Container Instances[7]	✓	✓	✓	✓	✓	✓
	Container Registry	✓	✓	✓	✓	✓	✓
Networking	Application Gateway	✓	✓	✓	✓	✓	✓
	Azure Bastion	✓	✓	-	-	✓	✓
	Azure DDoS Protection[7]	✓	✓	✓	✓	✓	✓
	Azure DNS	✓	✓	✓	✓	✓	✓
	Azure ExpressRoute	✓	✓	✓	✓	✓	✓
	Azure Firewall	✓	✓	✓	✓	✓	✓
	Azure Firewall Manager	✓	-	-	-	-	✓
	Azure Front Door[7]	✓	✓	✓	✓	✓	✓

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

[7] Examination period for this offering / service for Azure was from April 1, 2019 to March 31, 2020, while the examination period for Azure Government was from October 1, 2019 to March 31, 2020.

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[5]			
		Azure	Azure Government	Q4 FY19	Q1 FY20	Q2 FY20	Q3 FY20
	Azure Internet Analyzer	✓	-	-	-	✓	✓
	Azure Private Link	✓	✓	-	-	✓	✓
	Azure Web Application Firewall	✓	✓	-	-	✓	✓
	Content Delivery Network	✓	-	✓	✓	✓	✓
	Load Balancer	✓	✓	✓	✓	✓	✓
	Network Watcher	✓	✓	✓	✓	✓	✓
	Traffic Manager	✓	✓	✓	✓	✓	✓
	Virtual Network	✓	✓	✓	✓	✓	✓
	VPN Gateway	✓	✓	✓	✓	✓	✓
	Virtual WAN	✓	✓	-	-	✓	✓
Storage	Azure Archive Storage[7]	✓	✓	✓	✓	✓	✓
	Azure Backup	✓	✓	✓	✓	✓	✓
	Azure Data Box	✓	✓	-	-	✓	✓
	Azure Data Lake Storage Gen1	✓	-	✓	✓	✓	✓
	Azure File Sync[7]	✓	✓	✓	✓	✓	✓
	Azure HPC Cache	✓	-	-	-	✓	✓
	Azure Import/Export	✓	✓	✓	✓	✓	✓
	Azure Site Recovery	✓	✓	✓	✓	✓	✓
	Azure Storage (Blobs (including Azure Data Lake Storage Gen2), Disks, Files, Queues, Tables) including Cool and Premium	✓	✓	✓	✓	✓	✓
	Azure Ultra Disk	✓	-	-	-	✓	✓
	StorSimple	✓	✓	✓	✓	✓	✓
Databases	Azure API for FHIR	✓	-	✓	✓	✓	✓
	Azure Cache for Redis	✓	✓	✓	✓	✓	✓

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[5]			
		Azure	Azure Government	Q4 FY19	Q1 FY20	Q2 FY20	Q3 FY20
	Azure Cosmos DB	✓	✓	✓	✓	✓	✓
	Azure Database for MariaDB[7]	✓	✓	✓	✓	✓	✓
	Azure Database for MySQL[7]	✓	✓	✓	✓	✓	✓
	Azure Database for PostgreSQL[7]	✓	✓	✓	✓	✓	✓
	Azure Database Migration Service	✓	-	✓	✓	✓	✓
	Azure SQL Database	✓	✓	✓	✓	✓	✓
	Azure Synapse Analytics	✓	✓	✓	✓	✓	✓
	SQL Server on Virtual Machines	✓	✓	✓	✓	✓	✓
Developer Tools	Azure DevTest Labs	✓	✓	✓	✓	✓	✓
	Azure Lab Services	✓	✓	✓	✓	✓	✓
Analytics	Azure Analysis Services	✓	✓	✓	✓	✓	✓
	Azure Data Explorer	✓	✓	✓	✓	✓	✓
	Azure Data Share	✓	-	-	-	✓	✓
	Azure Stream Analytics[7]	✓	✓	✓	✓	✓	✓
	Data Catalog	✓	-	✓	✓	✓	✓
	Data Factory	✓	✓	✓	✓	✓	✓
	Data Lake Analytics	✓	-	✓	✓	✓	✓
	HDInsight	✓	✓	✓	✓	✓	✓
	Power BI Embedded	✓	✓	✓	✓	✓	✓
AI + Machine Learning	AI Builder	✓	-	-	-	✓	✓
	Azure Bot Service	✓	✓	✓	✓	✓	✓
	Azure Open Datasets	✓	-	-	-	✓	✓
	Azure Machine Learning	✓	-	✓	✓	✓	✓
	Cognitive Services	✓	✓	✓	✓	✓	✓

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[5]			
		Azure	Azure Government	Q4 FY19	Q1 FY20	Q2 FY20	Q3 FY20
	Cognitive Services: Anomaly Detector	✓	-	-	-	✓	✓
	Cognitive Services: Computer Vision	✓	✓	✓	✓	✓	✓
	Cognitive Services: Content Moderator	✓	✓	✓	✓	✓	✓
	Cognitive Services: Custom Vision	✓	-	✓	✓	✓	✓
	Cognitive Services: Face	✓	✓	✓	✓	✓	✓
	Cognitive Services: Form Recognizer	✓	-	-	-	✓	✓
	Cognitive Services: Language Understanding	✓	✓	✓	✓	✓	✓
	Cognitive Services: Translator	✓	✓	✓	✓	✓	✓
	Cognitive Services: Personalizer	✓	-	-	-	✓	✓
	Cognitive Services: QnA Maker	✓	-	✓	✓	✓	✓
	Cognitive Services: Speech Services[7]	✓	✓	✓	✓	✓	✓
	Cognitive Services: Text Analytics	✓	✓	✓	✓	✓	✓
	Cognitive Services: Video Indexer	✓	-	✓	✓	✓	✓
	Machine Learning Studio (Classic)	✓	-	✓	✓	✓	✓
	Microsoft Genomics	✓	-	✓	✓	✓	✓
	Microsoft Healthcare Bot	✓	-	✓	✓	✓	✓
Internet of Things	Azure IoT Central	✓	-	✓	✓	✓	✓
	Azure IoT Hub	✓	✓	✓	✓	✓	✓
	Event Grid	✓	✓	✓	✓	✓	✓
	Event Hubs	✓	✓	✓	✓	✓	✓
	Notification Hubs	✓	✓	✓	✓	✓	✓
	Time Series Insights	✓	-	-	✓	✓	✓

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[5]			
		Azure	Azure Government	Q4 FY19	Q1 FY20	Q2 FY20	Q3 FY20
	Windows 10 IoT Core Services	✓	-	-	-	✓	✓
Integration	API Management	✓	✓	✓	✓	✓	✓
	Logic Apps	✓	✓	✓	✓	✓	✓
	Service Bus	✓	✓	✓	✓	✓	✓
Identity	Azure Active Directory	✓	✓	✓	✓	✓	✓
	Azure Active Directory B2C	✓	-	✓	✓	✓	✓
	Azure Active Directory Domain Services	✓	-	✓	✓	✓	✓
	Azure Information Protection	✓	✓	✓	✓	✓	✓
Management and Governance	Automation	✓	✓	✓	✓	✓	✓
	Azure Advisor	✓	✓	✓	✓	✓	✓
	Azure Blueprints	✓	-	-	✓	✓	✓
	Azure Lighthouse	✓	✓	-	-	✓	✓
	Azure Managed Applications[8]	✓	✓	-	✓	✓	✓
	Azure Migrate	✓	✓	✓	✓	✓	✓
	Azure Monitor	✓	✓	✓	✓	✓	✓
	Azure Policy	✓	✓	✓	✓	✓	✓
	Azure Resource Graph	✓	✓	-	-	✓	✓
	Azure Resource Manager (ARM)[6]	✓	✓	✓	✓	✓	✓
	Cloud Shell[7]	✓	✓	✓	✓	✓	✓
	Microsoft Azure Portal[6]	✓	✓	✓	✓	✓	✓
	Scheduler	✓	✓	✓	✓	✓	✓
Security	Azure Advanced Threat Protection[7]	✓	✓	✓	✓	✓	✓
	Azure Dedicated HSM[7]	✓	✓	✓	✓	✓	✓

[8] Examination period for this offering / service for Azure was from July 1, 2019 to March 31, 2020, while the examination period for Azure Government was from October 1, 2019 to March 31, 2020.

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[5]			
		Azure	Azure Government	Q4 FY19	Q1 FY20	Q2 FY20	Q3 FY20
	Azure Security Center	✓	✓	✓	✓	✓	✓
	Azure Sentinel	✓	-	-	✓	✓	✓
	Customer Lockbox for Microsoft Azure	✓	-	-	-	✓	✓
	Key Vault	✓	✓	✓	✓	✓	✓
	Multi-Factor Authentication	✓	✓	✓	✓	✓	✓
Media	Azure Media Services	✓	✓	✓	✓	✓	✓
Web	Azure Cognitive Search[7]	✓	✓	✓	✓	✓	✓
	Azure SignalR Service	✓	-	✓	✓	✓	✓
Internal Supporting Services[6,9]		✓	✓	✓	✓	✓	✓

Offering	Cloud Environment Scope		Examination Period Scope[5]			
	Azure	Azure Government	Q4 FY19	Q1 FY20	Q2 FY20	Q3 FY20
Microsoft Online Services						
Intune[7]	✓	✓	✓	✓	✓	✓
Microsoft Cloud App Security[7]	✓	✓	✓	✓	✓	✓
Microsoft Defender Advanced Threat Protection[7]	✓	✓	✓	✓	✓	✓
Microsoft Graph[7]	✓	✓	✓	✓	✓	✓
Microsoft Managed Desktop	✓	-	✓	✓	✓	✓
Microsoft Stream	✓	-	✓	✓	✓	✓
Microsoft Threat Experts	✓	-	-	-	✓	✓

[9] Azure Government scope boundary for internal services: AsimovEventForwarder, Azure Networking, Azure RBAC Ibiza UX (Hosted extension), Azure Security Monitoring (ASM SLAM), Azure Stack Bridge, Azure Stack Edge Service, Azure Watson, CEDIS-Active Directory Domain Services, CEDIS-Active Directory Federation Services, CEDIS-Azure Active Directory, Cloud Data Ingestion, Compute Manager, dSCM, dSMS, dSTS, Geneva Actions, Geneva Warm Path, IAM - Management Admin UX, OneDS Collector, PilotFish, Protection Center, WANetMon, Windows Azure Jumpbox, Workflow. The coverage period for internal services for both Azure and Azure Government is Q4 FY19 through Q3 FY20 except for those specified with shorter coverage periods in the *Internal Supporting Services* subsection herein.

Offering	Cloud Environment Scope		Examination Period Scope[5]			
	Azure	Azure Government	Q4 FY19	Q1 FY20	Q2 FY20	Q3 FY20
Microsoft Threat Protection[7]	✓	✓	✓	✓	✓	✓
Power Apps	✓	✓	✓	✓	✓	✓
Power Automate	✓	✓	✓	✓	✓	✓
Power BI	✓	✓	✓	✓	✓	✓
Power Virtual Agents	✓	-	-	-	✓	✓

Offering	Cloud Environment Scope		Examination Period Scope[5]			
	Azure	Azure Government	Q4 FY19	Q1 FY20	Q2 FY20	Q3 FY20
Microsoft Dynamics 365						
Dynamics 365 AI Customer Insights	✓	-	✓	✓	✓	✓
Dynamics 365 Business Central	✓	-	✓	✓	✓	✓
Dynamics 365 Commerce	✓	-	✓	✓	✓	✓
Dynamics 365 Customer Engagement	✓	✓	✓	✓	✓	✓
Dynamics 365 Customer Service	✓	✓	✓	✓	✓	✓
Dynamics 365 Field Service	✓	✓	✓	✓	✓	✓
Dynamics 365 Finance	✓	-	✓	✓	✓	✓
Dynamics 365 Fraud Protection	✓	-	-	✓	✓	✓
Dynamics 365 Human Resources	✓	-	✓	✓	✓	✓
Dynamics 365 Marketing	✓	-	-	✓	✓	✓
Dynamics 365 Portals	✓	✓	✓	✓	✓	✓
Dynamics 365 Project Service Automation	✓	-	✓	✓	✓	✓
Dynamics 365 Sales	✓	✓	✓	✓	✓	✓
Dynamics 365 Supply Chain Management	✓	-	-	-	✓	✓

Locations Covered by this Report

Azure production infrastructure is located in globally distributed datacenters. These datacenters 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:

Domestic Datacenters

West US
• Santa Clara, CA (BY1/2/3/4/5[10]/21/22/24[10]/30[11])
• San Jose, CA (SJC31)

West US 2
• Quincy, WA (CO1/2, MWH01/02[10]/03[10])

West Central US
• Cheyenne, WY (CYS01/04/05[10])

Central US
• Des Moines, IA (DM1/2/3, DSM05/06[10]/08[10])

USGOV Iowa
• Des Moines, IA (DM2)

North Central US
• Chicago, IL (CH1/3/4[10], CHI20/21[10])

USGOV Arizona
• Phoenix, AZ (PHX20/21[10])

South Central US
• San Antonio, TX (SN1/2/3/4/6, SAT09[11])

USGOV Texas
• San Antonio, TX (SN5)

East US
• Bristow, VA (BLU)
• Reston, VA (BL4/31[11])
• Sterling, VA (BL20)
• Ashburn, VA (BL2/3/5/6/7/21[10]/22[10]/23[10]/30)
• Manassas, VA (MNZ20[10])

East US 2
• Boydton, VA (BN1/3/4/6/7[10]/8[10]/14[10])

USGOV Virginia
• Boydton, VA (BN1)

USDoD East
• Boydton, VA (BN3)

International Datacenters

Canada East
• Quebec, Canada (YQB20)

Canada Central
• Toronto, Canada (YTO20/21[10])

Brazil South
• Campinas, Brazil (CPQ01/02/20)
• Sao Paulo, Brazil (GRU)

Brazil Southeast
• Rio de Janeiro, Brazil (RIO01)

Brazil Northeast
• Fortaleza, Brazil (FOR01)

East Asia
• Hong Kong (HK1/2, HKG20/21[10])

West India
• Mumbai, India (BOM01)

Central India
• Dighi, India (PNQ01)

South India
• Ambattur, India (MAA01)

Japan West
• Osaka, Japan (OSA01/02/20/21[10]/22[10])

Japan East
• Tokyo, Japan (KAW, TYO01/20/21/22/31[10])

[10] Examination period for this datacenter was from October 1, 2019 to March 31, 2020.

[11] Examination period for this datacenter was from July 1, 2019 to March 31, 2020.

International Datacenters

Chile Central
• Santiago, Chile (SCL01)

West Europe
• Amsterdam, Netherlands (AM1/2/3, AMS04/05/06/07[10]/20/21[11]/23[10])
• Luxembourg A: SecureIT (LUA[10])

East Europe
• Vienna, Austria (VIE)

North Europe
• Dublin, Ireland (DB3/4/5, DUB06/07/08/11[10]/20/21[10]/24/31[10])

North Europe 2
• Vantaa, Finland (HEL01)

UK North
• Durham, United Kingdom (MME20)

UK South
• London, United Kingdom (LON21/22[11]/23[11]/24[11])

UK South 2
• London, United Kingdom (LON20)

UK West
• Cardiff, United Kingdom (CWL20)

France Central
• Paris, France (PAR20/21/22/23[10])

France South
• Marseille, France (MRS20)

Germany North
• Berlin, Germany (BER20[12])

Germany West Central
• Frankfurt, Germany (FRA21[12])

Switzerland West
• Geneva, Switzerland (GVA20[11])

Switzerland North
• Zurich, Switzerland (ZRH20[11])

Southeast Asia
• Singapore (SG1/2/3, SIN20)

Southeast Asia 2
• Cyberjaya, Malaysia (KUL01)

Korea South
• Busan, South Korea (PUS01/20)

Korea Central
• Seoul, South Korea (SEL20/21[11])

UAE Central
• Abu Dhabi (AUH20)

UAE North
• Dubai (DXP20)

Australia East
• Macquarie Park, Australia (SYD03)
• Sydney, Australia (SYD21/22/23[10]/25[10])

Australia Southeast
• Melbourne, Australia (MEL01/20[10]/21[10])

Australia Central
• Canberra, Australia (CBR20/21)

South Africa North
• Johannesburg, South Africa (JNB20/21/22)

South Africa West
• Cape Town, South Africa (CPT20)

Norway East
• Oslo, Norway (OSL20[10])

Norway West
• Stavanger, Norway (SVG20[10])

[12] Examination period for this datacenter was from May 1, 2019 to March 31, 2020.

Edge Sites

- Ashburn, VA (ASH)
- Athens, Greece (ATH01)
- Atlanta, GA (ATA)
- Auckland, New Zealand (AKL01)
- Bangkok, Thailand (BKK30)
- Barcelona, Spain (BCN30)
- Berlin, Germany (BER30)
- Boston, MA (BOS01/31[13])
- Brisbane, Australia (BNE01)
- Brussels, Belgium (BRU30)
- Bucharest, Romania (BUH01)
- Budapest, Hungary (BUD01)
- Busan, South Korea (PUS03)
- Cape Town, South Africa (CPT02)
- Chicago, IL (CHG)
- Copenhagen, Denmark (CPH30)
- Dallas, TX (DAL)
- Denver, CO (DEN02)
- Dubai, United Arab Emirates (DXB30)
- Frankfurt, Germany (FRA)
- Geneva, Switzerland (GVA30[13])
- Helsinki, Finland (HEL03)
- Hong Kong (HKB)
- Honolulu, HI (HNL01)
- Houston, TX (HOU01)
- Hyderabad, India (HYD30[14])
- Jakarta, Indonesia (JKT30[13])
- Johannesburg, South Africa (JNB02)
- Kuala Lumpur, Malaysia (KUL30)
- Las Vegas, NV (LAS01)
- Lisbon, Portugal (LIS01)
- Los Angeles, CA (LAX)
- Lagos, Nigeria (LOS30[13])
- Madrid, Spain (MAD30)
- Manchester, United Kingdom (MAN30)
- Manila, Philippines (MNL30)
- Marseille, France (MRS01)
- Munich, Germany (MUC30[13])
- Nairobi, Kenya (NBO30[13])
- Queretaro, Mexico (MEX30)
- Miami, FL (MIA)
- Milan, Italy (MIL30)
- Montreal, Canada (YMQ01)
- Mumbai, India (BOM02)
- New Delhi, India (DEL01)
- Newark, NJ (EWR30)
- Osaka, Japan (OSA31[13])
- Oslo, Norway (OSL30[13])
- New York City, NY (NYC)
- Paris, France (PAR02/PRA)
- Perth, Australia (PER01/30[13])
- Phoenix, AZ (PHX01)
- Portland, OR (PDX31[14])
- Prague, Czech Republic (PRG01)
- Sao Paulo, Brazil (SAO03[13])
- San Jose, CA (SJC)
- Santiago, Chile (SCL30)
- Seattle, WA (WST)
- Seoul, South Korea (SLA)
- Sofia, Bulgaria (SOF01)
- Stockholm, Sweden (STO)
- Taipei, Taiwan (TPE30)
- Tokyo, Japan (TYA/TYB)
- Toronto, Canada (YTO01)
- Vancouver, Canada (YVR01)
- Warsaw, Poland (WAW01)
- Zagreb, Croatia (ZAG30)
- Zurich, Switzerland (ZRH)

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 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

[13] Examination period for this edge site was from October 1, 2019 to March 31, 2020.

[14] Examination period for this edge site was from July 1, 2019 to March 31, 2020.

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, Microsoft Enterprise Enrollment Agreement (Volume Licensing - Online Services 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 are communicated in Azure's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of various Azure services and offerings.

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.

Office of Legal Compliance - Board of Directors and Senior Leadership

The Office of Legal Compliance (OLC) 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

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

IA specialization area leaders determine high-priority risks across the company, including 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.

Office of Legal Compliance / Internal Audit / Risk Management - Risk Responsibility

The responsibility for risk is distributed throughout the organization based on the individual group's services. OLC, 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.

Office of Legal Compliance - Business Conduct Hotline

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

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

Internal Audit

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

Information and Communication

An annual process exists to set objectives and commitments among all executives and is rolled down to employees. These commitments and objectives are filtered down to team members through the annual and 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. **Account Data** is information about payment instruments. This type of data is not stored in the Azure platform.

6. **Public Personal Data** is publicly available personal information that Microsoft obtains from external sources.

7. **End User Pseudonymous Identifiers (EUPI)** are identifiers created by Microsoft, tied to the user of a Microsoft service.

8. **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.

9. **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.

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

Data Ownership

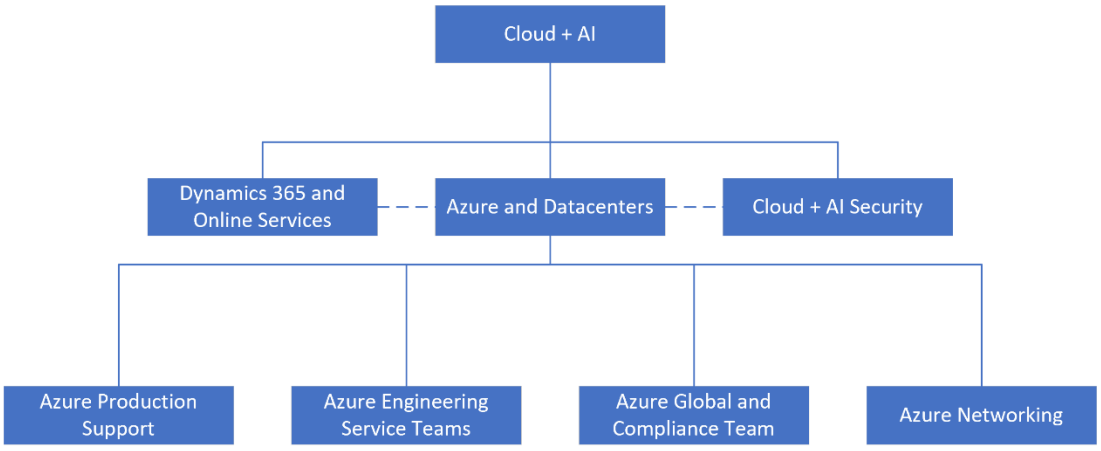
Microsoft does not inspect, approve, or monitor applications that customers deploy to Azure. Moreover, Microsoft does not know what kind of data customers choose to store in Azure. Microsoft does not claim data ownership over the customer information entered into Azure. Azure's Agreement states, "Customers 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 Data 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:



Online Services

Online Services teams manage the service lifecycle of the finished SaaS services that leverage the underlying Azure platform and datacenter infrastructure. They are responsible for the development of new features, operational support, and escalations.

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 Secure Development Lifecycle (SDL). They also perform security reviews and provide security guidance for the datacenters. This team consists of personnel responsible for:

- Secure 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

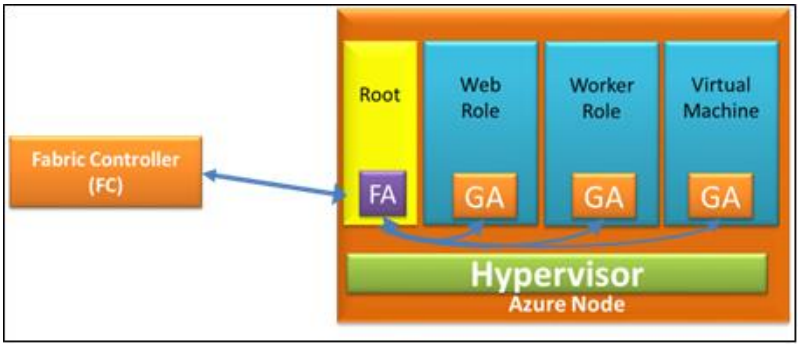
The Networking team is responsible for implementing, monitoring and maintaining the Microsoft network. This team consists of personnel responsible for:

- 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 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

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

- 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.
- App Service: Mobile Apps: Mobile Apps 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.
- 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 (CLI) tools running on any OS, source code control driven deployments, as well as from within the Visual Studio Integrated Development Environment (IDE).

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 HTTP endpoints accessible by mobile and Internet of Things (IoT) devices.

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.

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.

Cloud Services: Cloud Services is a PaaS service designed to support applications that are scalable, reliable, and inexpensive to operate. 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 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.

Virtual Machines: 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.

Virtual Machine Scale Sets: 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.

Containers

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 (ARO): 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.

Container Instances: Container Instances enables the creation of containers as first-class objects in Azure, without requiring VM management and without enforcing any prescriptive application model. 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.

Container Registry: 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 App Service, Batch, Azure Service Fabric, and others. Developers can manage the configuration of apps isolated from the configuration of the hosting environment. 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.

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 RDP and 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 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 DNS domains that provides name resolution by using Microsoft Azure infrastructure. Azure DNS lets customers host their Domain Name System (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 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 Internet Analyzer: Azure Internet Analyzer is a client-side measurement platform that tests how changes to customer's networking infrastructure impact their client's / end-user's performance. Internet Analyzer uses a small JavaScript client embedded in the customer's web application to measure the latency from their end-users to customer selected set of network destinations (endpoints). Internet Analyzer allows customers to set up multiple side-by-side tests, allowing to evaluate a variety of scenarios as their infrastructure and needs evolve. It provides custom and preconfigured endpoints, providing a customer both the convenience and flexibility to make trusted performance decisions for their end-users.

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 Web Application Firewall: Azure Web Application Firewall (WAF) 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.

Content Delivery Network: 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.

Load Balancer: 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.

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 Network: 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.

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).

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.

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 (DPM). 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 (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 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 Import / Export: Azure Import / Export allows customers to securely transfer large amounts of data to Azure Blob Storage by shipping hard disk drives to an Azure datacenter. Customers can also use this service to transfer data from Azure Blob Storage to hard disk drives and ship to their on-premises site. This service is suitable in situations where customers want to transfer several TBs of data to or from Azure, but uploading or downloading over the network is not feasible due to limited bandwidth or high network costs.

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 ACLs, and Hadoop Distributed File System (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 Virtual Hard Disk (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.

- Files: Files offer shared storage for applications using the Server Message Block (SMB) protocol or REST protocol. Files can be used to completely replace or supplement traditional on-premises file servers or NAS devices. Applications running in Azure VMs, Cloud Services or from on-premises clients can access Files using SMB or REST.

- 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.

- 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 Ultra Disk: Azure Ultra Disk offers high throughput, high Input / Output Operations Per Second (IOPS), 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 Ultra Disks are suited for data-intensive workloads such as SAP HANA, top tier databases, and transaction-heavy workloads.

StorSimple: StorSimple is a hybrid cloud storage solution for primary storage, archiving, and disaster recovery. StorSimple optimizes total storage costs and data protection. It includes an on-premises Storage Area Network (SAN) solution that is a bottomless file server using Azure Blob Storage. StorSimple automatically arranges data in logical tiers based on current usage, age, and relationship to other data. Data that is most active is stored locally, while less active and inactive data is automatically migrated to the cloud. A StorSimple appliance is managed via the Azure Portal.

Databases

Azure API for FHIR: Azure API for FHIR 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 API for FHIR improves health technologies' interoperability and makes it easier to manage data.

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 Service Level Agreements (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 SQL Database: Azure SQL Database is a relational database service that lets customers rapidly create, extend, and scale relational applications into the cloud. Azure SQL Database 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 Database provides a familiar programming model based on T-SQL and supports existing SQL Server tools, libraries and APIs.

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, Data Factory, and Microsoft Power BI for a complete data-warehousing and business-intelligence solution in the cloud.

SQL Server on Virtual Machines: SQL Server on Virtual Machines enables customers to create a SQL Server in the cloud that they can control and manage. SQL Server on Virtual Machines offers a robust infrastructure for SQL Server by using Azure as a hosting environment for enterprise database applications. SQL Server is a

database for transactions, queries and analytics for Big Data solutions. SQL Server is not in scope of this SOC report.

Developer Tools

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 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.

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 (OLAP) 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 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 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 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 Factory: 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 (ETL / ELT) processes code free in an intuitive visual environment, and easily operationalize and manage the data pipelines at scale.

Data Lake Analytics: Data Lake Analytics is a distributed analytics service built on Apache Yet Another Resource Negotiator (YARN) 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 Azure Active Directory 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 Database, and Azure Synapse Analytics.

HDInsight: 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. HDInsight includes Apache Hbase, a columnar NoSQL database that runs on top of the Hadoop Distributed File System (HDFS). This supports large transactional processing (Online Transaction Processing (OLTP)) of non-relational data, enabling use cases like interactive websites or having sensor data written to Azure Blob Storage. 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, HDInsight includes Apache Spark, an open-source project in the Apache ecosystem that can run large-scale data analytics applications in memory. Lastly, HDInsight incorporates R Server for Hadoop, a scale-out implementation of one of the most popular programming languages for statistical computing and machine learning. HDInsight offers Linux clusters when deploying Big Data workloads into Azure.

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 Bot Service: Azure Bot Service helps developers build bots / intelligent agents and connect them to the communication channels their users are in. Azure 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 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 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 & ML Ops. It is open-source friendly and works with any Python framework, such as PyTorch, TensorFlow, or scikit-learn.

Cognitive Services: Cognitive 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.

Cognitive Services: Anomaly Detector: Cognitive Services: 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.

Cognitive Services: Computer Vision: Cognitive Services: Computer 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.

Cognitive Services: Content Moderator: Cognitive Services: Content Moderator 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.

Cognitive Services: Custom Vision: Cognitive Services: Custom Vision is a cognitive 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.

Cognitive Services: Face: Cognitive Services: Face is a service that has two main functions - face detection with attributes and face recognition. It provides customers 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.

Cognitive Services: Form Recognizer: Cognitive Services: Form Recognizer is a cognitive 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. Form Recognizer is comprised of custom models, the prebuilt receipt model, and the layout API. Customers can call Form Recognizer models by using a REST API to reduce complexity and integrate it into a workflow or an application.

Cognitive Services: Language Understanding: Cognitive Services: 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.

Cognitive Services: Translator: Cognitive Services: 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.

Cognitive Services: Personalizer: Cognitive Services: 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. Personalizer collects and uses real-time information customers provide about content and context in order to select the most relevant content. 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.

Cognitive Services: QnA Maker: Cognitive Services: QnA Maker is a cognitive service 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.

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

Cognitive Services: Text Analytics: Cognitive Services: Text Analytics is a cloud-based service that provides advanced natural language processing over raw text, and includes five main functions: sentiment analysis, key phrase extraction, named entities recognition, linked entities, and language detection.

Cognitive Services: Video Indexer: Cognitive Services: 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.

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

Microsoft Healthcare Bot: Microsoft Healthcare 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.

Internet of Things

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're 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.

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

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.

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 (APNs), Firebase Cloud Messaging (FCM) service, Windows Push Notification Service (WNS), Microsoft Push Notification Service (MPNS), 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.

Time Series Insights: 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.

Windows 10 IoT Core Services: Windows 10 IoT Core Services is a cloud subscription-based service that provides essential aids needed to commercialize a device on Windows 10 IoT Core. Through this subscription, OEMs have access to support channel, along with services to publish device updates and assess device health. Windows 10 IoT Core services offers monthly security and reliability updates, keeping devices stable and secure and utilizes Device Update Center to control device updates using the same content distribution network that is used by millions of customers to manage Windows updates.

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.

Logic Apps: 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, Office 365, Twitter, Dropbox, Google services, and more.

Service Bus: 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 (FIFO) messaging, and publish / subscribe capabilities. Service Bus uses Advanced Message Queuing Protocol (AMQP), Service Bus Messaging Protocol (SBMP), and HTTP as its primary protocols.

Identity

Azure Active Directory (AAD): 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. AAD comes in 3 editions: Free, Basic, and Premium. Self-service credentials management is a feature of AAD that allows Azure AD 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 AAD that provides the backend to support authentication and provisioning for AAD.

Azure Active Directory B2C: Azure Active Directory B2C extends Azure Active Directory 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.

Azure Active Directory Domain Services: Azure Active Directory 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. Customers can consume these domain services without the need to deploy, manage, and patch domain controllers in the cloud. Azure Active Directory Domain Services integrates with the existing Azure Active Directory tenant, thus making it possible for users to log in using their corporate credentials.

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

Management and Governance

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 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: 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.

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.

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 Microsoft Online Services Customer Portal (MOCP). MOCP and MSA / Organizational Accounts and their associated authentication mechanisms are not in scope for this SOC report.

Scheduler: Scheduler lets customers invoke actions that call HTTP/S endpoints or post messages to an Azure Storage queue, Service Bus queue, or Service Bus topic on any schedule. It creates jobs that reliably call services either inside or outside of Azure and run those jobs right away, on a regular or irregular schedule, or at a future

date. Scheduler was retired in calendar year Q4 2019 with all of the service functionality moved to Logic Apps. However, this service continues to support existing customers until it is fully decommissioned.

Security

Azure Advanced Threat Protection: Azure Advanced Threat Protection (ATP) 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.

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

Azure Security Center: Azure Security Center 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.

Azure Sentinel: Azure 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. Azure 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.

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 Hardware Security Modules (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.

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.

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 Cognitive Search: Azure Cognitive 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 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.

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., Office 365 and Dynamics 365.

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.

Azure Networking: Azure Networking is used to provide all datacenter connectivity for Azure. Azure Networking is completely transparent to Azure customers who cannot interact directly with any physical network device. The Azure Networking 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 Azure Networking 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.

Azure Privileged Identity Management: Azure Privileged Identity Management lets customers manage, control and monitor their privileged identities and their access to resources in Azure AD, and in other Microsoft Online Services such as Office 365 or Microsoft Intune. Azure Privileged Identity Management allows customers to see which users are Azure AD administrators; enables on-demand, "just in time" administrative access to Microsoft Online Services like Office 365 and Intune; provides reports about administrator access history and changes in administrator assignments; provides alerting about access to a privileged role. It can manage the built-in Azure AD organizational roles, such as Global Administrator, Billing Administrator, Service Administrator, User Administrator and Password Administrator.

Azure RBAC Ibiza UX (Hosted extension): Azure RBAC Ibiza UX (Hosted extension) covers the Access Control (IAM) experience for Azure resources in the Ibiza portal. It supports operations like listing, granting, and revoking access to Azure resources, managing Azure RBAC custom roles, checking what access a principal has on an Azure resource, and more.

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 Manager (RDFE): 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 Service Management API (SMAPI). All requests from the user go through Azure Service Manager (RDFE) or the newer Azure Resource Manager (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 Edge Service[15]: 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 Watson: Azure Watson is an internal tool for service troubleshooting and crash dump analysis.

CEDIS - Active Directory Domain Services: CEDIS - Active Directory Domain Services provides Active Directory Domain Services (AD DS) for internal Microsoft customers like Azure, Online Services, and Microsoft Retail in the Public and Government cloud environments.

CEDIS - Active Directory Federation Services: CEDIS - ADFS manages an instance of ADFS for internal users of Microsoft in Public Azure and the National clouds.

CEDIS - Azure Active Directory: CEDIS - AAD manages an instance of AAD Connect for internal users of Microsoft in Public Azure and the National clouds. The services are limited to authorized access to low levels of the cloud environment only.

Cloud Data Ingestion: Cloud Data Ingestion (CDI) is a set of worker roles that reads sign-in and audit events from multiple sources like Evolved Security Token Service (eSTS), MSODS, IAM - Self Service Credentials Management Service, etc., and ingest them into the data processing pipeline for products like Identity Protection Center (IPC) and audit reports in the Ibiza portal. CDI also has a web role that manages Event Hubs and storage for all the services in the data processing pipeline.

Cognitive Services: Container Platform: Cognitive Services: Container Platform is the backend platform that hosts multiple Cognitive Services offerings.

Compute Manager: 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 (TM), Container Manager (CM) and Allocator.

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

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.

DesktopAnalytics: DesktopAnalytics provides enterprise customers with device telemetry data to obtain and maintain accurate customer details across Office and Windows.

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.

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

[15] Examination period for this service was from July 1, 2019 to March 31, 2020.

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.

Enterprise Data Platform[15]: Enterprise Data Platform is a data pipeline service that collects, analyzes and shares back value add telemetry to Microsoft Enterprise customers.

Enterprise Knowledge Graph[16]: Enterprise Knowledge Graph enables customers to build scalable knowledge solutions based on a flexible ontology and advanced conflation capability. This service was decommissioned in calendar year Q4 2019.

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 Office.

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

Hybrid Identity Service: Hybrid Identity Service (HIS) is the backend service for tunneling requests from the cloud to resources on-premises. Current products include Pass-through Authentication (PTA), which allows Evolved Security Token Service (EvoSTS) to authenticate users against Active Directory on-premises.

IAM - Management Admin UX: IAM - Management Admin UX is a stateless, UI-only extension to the Azure Management Portal that allows directory users in various administrative roles to manage all aspects of a lifecycle of objects in an Azure Active Directory (such as users, groups, applications, domains, policies etc.), in terms of creation, deletion, viewing and editing. It also enables access to various AAD features depending on the licensing level of the customer.

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.

OneDS Collector: OneDS Collector is the ingestion front end for the telemetry pipelines used by Microsoft Windows, Microsoft Office 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.

Pilotfish: Pilotfish is available to first-party customers (e.g., Office 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.

[16] Examination period for this service was from July 1, 2019 to September 30, 2019.

Protection Center: Protection Center is a cloud security service that uses state of the art machine learning to analyze 10 terabytes of behavioral and contextual data every day to detect and prevent attempts to attack organizations' Azure AD accounts.

TuringAtAzure: TuringAtAzure is an API service that allows Microsoft product teams to access Turing language models in their production scenario.

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 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 O365 SharePoint Online service.

Microsoft Online Services

Intune: 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 Cloud App Security (MCAS): Microsoft Cloud App Security 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. MCAS provides Shadow IT discovery, information protection to cloud applications, threat detection and in-session controls.

Microsoft Defender Advanced Threat Protection: Microsoft Defender Advanced Threat Protection is a complete endpoint security solution for preventative protection, post-breach detection, automated investigation, and response.

Microsoft Graph: Microsoft Graph exposes multiple APIs from Office 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 Azure Active Directory, Exchange Online as part of Office 365, SharePoint, OneDrive, OneNote, and Planner.
- Navigate between entities and relationships.
- Access intelligence and insights from the Microsoft cloud (for commercial users).

Microsoft Managed Desktop (MMD): Microsoft Managed Desktop (MMD) combines Microsoft 365 Enterprise with an IT-as-a-Service (ITaaS) 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 cognitive 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.

Microsoft Threat Experts: Microsoft Threat Experts 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.

Microsoft Threat Protection: Microsoft Threat Protection (MTP) is an integrated experience with AI and automation built in, that is built on best-in-class Microsoft 365 threat protection services and pools their collective knowledge and capabilities to accrue to something even better. It leverages and integrates these services' industry-leading prevention, detection, investigation, and response techniques to help secure attack vectors across users, endpoints, cloud apps, and data.

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 RP is an ARM resource provider, 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.

Power Virtual Agents: Power Virtual Agents 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 Dynamics 365

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 Business Central: Dynamics 365 Business Central, formerly known as Dynamics NAV, is Microsoft's Small and Medium Business (SMB) 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 Customer Engagement: Dynamics 365 Customer Engagement is a cloud-based customer relationship management (CRM) business solution that can help customers drive sales productivity and improve the value of marketing efforts through social insights, business intelligence, and campaign management. It includes a variety of applications such as Dynamics 365 for Sales, Dynamics 365 for Customer Service, Dynamics 365 for Project Service Automation, and Dynamics 365 for Field Service.

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

Dynamics 365 Portals: Dynamics 365 Portals is where users can log-in and view an aggregated list of their business apps across various partner services including PowerApps.

Dynamics 365 Project Service Automation: Dynamics 365 Project Service Automation (PSA) application helps organizations efficiently track, manage, and deliver project-based services, from the initial sale all the way to invoicing.

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.

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 (CIA) of information while complying with applicable legislative, regulatory, and contractual requirements.

The Information Security Program consists of the following components:

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

The Information Security Program is based on the International Organization of Standards (ISO) Codes of Practice for information security management ISO / IEC27001:2013 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 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. Secure Development Lifecycle
21. Security Assessment and Authorization
22. Software Change and Release Management
23. Third Party Management
24. Training and Awareness
25. Vulnerability Scanning and Patch Management

Microsoft Security Policy

Microsoft Security Policy (MSP) 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 MSP 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 Corporate, External, and Legal Affairs (CELA), 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 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 Standards of Business Conduct (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. 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

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.

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 Active Directory. Based on the configuration of a security group, any access request may either require explicit approval from the assigned security group owner or may be auto-approved for members of designated teams within Azure's organizational structure. 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 that require password-based authentication, if inactive for more than 90 days, are suspended until the appropriateness of continued access for these accounts is resolved.

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. Users are authenticated to access points using the AD domain credentials depending on where the production assets are located.

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.

Azure service teams have the ability to access production VMs utilizing RDP through the Azure Portal. This functionality is disabled by default and is only used in cases where the Just-in-Time (JIT) temporary access process cannot be used. Upon enabling RDP and creating a local account on an Azure VM, Cloud + AI Security team is notified of the non-standard account creation. Password parameters for such local accounts are governed by the OS baseline - if password parameters are overwritten, they are refreshed back to OS baseline password parameters every 30 days. Local accounts created on Azure subscriptions using the Azure Portal automatically expire based on the expiration set during account creation.

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 review 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 Directory Services 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 ten 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.

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 and revocation) in accordance with established key management procedures.

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.

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

Data Protection Services

The Data Protection Services (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.

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 Databases 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 Database detects the failure and fails over to the secondary replica. In case of a physical loss of the replica, Azure SQL Database 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 Database 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 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 (CA). 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 Representational State Transfer (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 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.

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 and hot fixes, 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.

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. 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.

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, Access Control Lists (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 Secure Development Lifecycle (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. Azure service teams track and complete their SDL compliance twice a year.

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. Permission to make changes to the source code is provided by granting write access to the source code branches, which limits the access to confined project boundaries per job responsibilities. In addition, source code builds are scanned for malware prior to production release.

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

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.

Azure has established an Audit Log Management policy, which restricts the log and monitor access to only authorized staff with a business need to access such systems. These logging servers follow the same process as defined in the Operator Access section above.

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.

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. Synthetic Transaction (STX) testing is the framework designed to support automated testing of Azure on-premises platform components in the service environment. The framework is used by component teams to test and alert upon failures in operation.

8. OpsView system is the framework designed to support the on-premises Multi-Factor Authentication service platform. Custom scripts have been implemented that are initiated by OpsView to provide logging and alerting capabilities upon detection of breaches or attempts to breach the MFA platform trust boundaries. Qualys and OpsView are collectively used to monitor these events. The event and warning logs are examined for anomalous behavior either through an automated alert system or manually, when necessary, and appropriate actions are taken in a timely manner.

9. HP ArcSight system is implemented to manage the authentication logs for the on-premises Multi-Factor Authentication service platform. The authentication logs capture all interactive logins and are sent to HP ArcSight through Syslogs that are managed by the CDOC team.

10. Pilotfish K9 system is implemented to manage the authentication logs for the on-premises Multi-Factor Authentication service platform. The authentication logs capture all interactive logins and are sent through Syslogs that are managed by the CDOC and Pilotfish teams.

11. 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 (USN) 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.

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.

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, Cyber Defense Operations Center (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 Azure Active Directory Graph API for programmatic access to Azure Active Directory through REST API endpoints. Applications can use the Graph API to perform 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 Azure Active Directory 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.

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).

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., Remote Desktop Protocol (RDP) or Secure Shell (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.

Azure Scheduler and Logic Apps allow 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 Storage Account Key (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 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 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 Business Impact Analysis, 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 (NTDA) 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, which is used 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 Service Resiliency (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 (GM) and CELA, and sign a Source Code Licensing Agreement.

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

Asset Management

Azure assets are classified in accordance with Microsoft Online Services Classification guidelines. The classification process is owned by the Azure Global Ecosystem and Compliance 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. On a monthly basis, the Azure Inventory team checks for completeness and accuracy of the inventory to ensure that it represents the Azure production environment appropriately.

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 Service Level Agreements (SLAs) available on the following website: https://www.microsoft.com/en-us/licensing/product-licensing/products.

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 Online Services 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 *(*AUP), 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 are communicated through the Microsoft Trust Center (https://www.microsoft.com/en-us/trustcenter/). Additionally, description of the services and the key components 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.

Microsoft Security Response Center (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. Customers and other third parties can report suspected vulnerabilities by emailing secure@microsoft.com.

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 Resource Provider (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 during the Azure Fundamentals (formerly through Service Health Review (SHR)) 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.

Relationship between CCM Criteria, Description Sections, and Trust Services Criteria

The description sections and the trust services criteria address the CCM criteria as follows:

CCM Area	Relevant Description Section	Trust Services Criteria
Application & Interface Security	Security Organization - Information Security Program, Data Security, Software Development, Logical Access, Communications, Processing Integrity	CC6.1, CC6.2, CC6.6, CC8.1, PI1.2, PI1.3, PI1.4, PI1.5
Audit Assurance & Compliance	Security Organization - Information Security Program	CC3.2, CC3.3, CC4.1, CC4.2

CCM Area	Relevant Description Section	Trust Services Criteria
Business Continuity Management & Operational Resilience	Security Organization - Information Security Program, Data Security, Change Management, Incident Management, Physical and Environmental Security, Communications, Business Continuity and Resiliency	CC1.1, CC1.4, CC2.3, CC3.2, CC3.3, CC5.1, CC5.2, CC4.1, CC4.2, CC7.2, A1.1, A1.2, A1.3
Change Control & Configuration Management	Security Organization - Information Security Program, Operator Access, Change Management, Software Development, Physical and Environmental Security, Baseline Configuration	CC6.2, CC6.4, CC6.5, CC6.8, CC8.1, CC8.1
Data Security & Information Lifecycle Management	Security Organization - Information Security Program, Operator Access, Data Security, Change Management, Software Development, Asset Management, Communications	C1.1, C1.2, CC2.2, CC2.3, CC3.2, CC3.3, CC6.1, CC6.6, CC6.7, CC8.1, PI1.4
Datacenter Security	Operator Access, Data Security, Physical and Environmental Security, Logical Access, Asset Management	CC3.2, CC3.3, CC6.1, CC6.4, CC6.5, CC6.7
Encryption & Key Management	Operator Access, Data Security, Logical Access	CC6.6, CC6.7
Governance and Risk Management	Security Organization - Information Security Program, Physical and Environmental Security, Baseline Configuration	CC1.3, CC1.5, CC2.2, CC2.3, CC3.1, CC3.2, CC3.3, CC7.3, CC7.4, CC7.5
Human Resources	Security Organization - Information Security Program	CC1.1, CC1.4, CC2.2, CC2.3, CC4.1, CC4.2, CC5.1, CC5.2, CC6.3, CC6.4, CC6.5, CC6.6, CC7.3, CC7.4, CC7.5
Identity & Access Management	Security Organization - Information Security Program, Operator Access, Data Security, Change Management, Software Development, Vulnerability Management, Physical and Environmental Security, Logical Access, Communications, Baseline Configuration	CC3.2, CC3.3, CC6.1, CC6.2, CC8.1
Infrastructure & Virtualization Security	Security Organization - Information Security Program, Operator Access, Data Security, Change Management, Software Development, Vulnerability Management, Logical Access, Business Continuity and Resiliency, Communications, Baseline Configuration	A1.1, A1.2, CC4.1, CC4.2, CC6.6, CC7.2, CC7.3, CC7.4, CC7.5

CCM Area	Relevant Description Section	Trust Services Criteria
Interoperability & Portability	Operator Access, Data Security, Logical Access, Communications	-
Mobile Security	*N/A - Microsoft Azure does not support mobile devices*	
Security Incident Management, E-Discovery & Cloud Forensics	Security Organization - Information Security Program, Incident Management, Communications	CC2.2, CC2.3, CC4.1, CC4.2, CC6.4, CC6.5, CC7.2, CC7.3, CC7.4, CC7.5. CC9.2
Supply Chain Management, Transparency and Accountability	Security Organization - Information Security Program, Operator Access, Change Management, Software Development, Business Continuity and Resiliency, Communications	CC2.2, CC2.3, CC6.4, CC6.5, CC9.2
Threat and Vulnerability Management	Software Development, Vulnerability Management, Communications	CC6.6, CC6.8, CC7.1, CC7.2, CC8.1

Relationship between Trust Services Criteria and Description Sections

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

Relationship between CCM Criteria and Description Sections

Refer to Part B in Section IV of this report for the CCM Criteria and the related control activities that cover those criteria.

Relationship between C5 Objectives and Description Sections

Refer to Part C in Section IV of this report for the C5 objectives and the related control activities that cover those objectives.

Section IV: Information Provided by Independent Service Auditor Except for Control Activities and Criteria Mappings

Section IV: Information Provided by Independent Service Auditor Except for Control Activities and Criteria Mappings

Introduction

This report on the description of the system of Microsoft Corporation ("Microsoft") related to in-scope services and offerings for Microsoft Azure, Microsoft Dynamics 365, and Microsoft datacenters ("Azure") for Azure and Azure Government cloud environments, is intended to provide user entities and their auditors with information for their evaluation of the effect of Microsoft's controls on the user entity's internal controls throughout the period April 1, 2019 to March 31, 2020.

This section presents the following information provided by Microsoft:

- The trust services criteria, the CCM criteria, and the objectives set forth in C5
- The controls established and specified by Microsoft to achieve the criteria for security, availability, processing integrity and confidentiality ("applicable trust services criteria"), the CCM criteria, and the objectives set forth in C5

Also included in this section is the following information provided by Deloitte & Touche LLP:

- A description of the tests performed by Deloitte & Touche LLP to determine whether Microsoft's controls were operating with sufficient effectiveness to achieve the applicable trust services criteria, the CCM criteria, and the objectives set forth in C5. Deloitte & Touche LLP determined the nature, timing, and extent of the testing performed
- The results of Deloitte & Touche LLP's tests of controls

Our examination was restricted to the applicable trust services criteria, the CCM criteria, the objectives set forth in C5, the related controls specified by Microsoft and testing procedures in Section IV of this report, and were not extended to procedures in effect at user entities.

It is each user's responsibility to evaluate the information included in this report in relation to internal controls in place at individual user entities to obtain an understanding and to assess control risk at the user entities. The controls at user entities and Microsoft's controls should be evaluated together. If effective user entity controls are not in place, Microsoft's controls may not compensate for such weaknesses.

Our examination included corroborative inquiry of the appropriate management, supervisory and staff personnel, inspection of documents and records, observation of activities and operations, and re-performance tests of controls performed by Microsoft. Our tests were performed on controls as they existed during the period April 1, 2019 to March 31, 2020, and were applied to those controls relating to the applicable trust services criteria, the CCM criteria, and the objectives set forth in C5 specified by Microsoft.

The description of controls is the responsibility of Microsoft's management. Our responsibility is to express an opinion about whether:

a. The Description fairly presents the system that was designed and implemented throughout the period April 1, 2019 to March 31, 2020.
b. The controls stated in the Description were suitably designed to provide reasonable assurance that the applicable trust services criteria, the CCM criteria, and the objectives set forth in C5 would be met if the

controls operated effectively throughout the period April 1, 2019 to March 31, 2020.

c. The controls operated effectively to provide reasonable assurance that the applicable trust services criteria, the CCM criteria, and the objectives set forth in C5 were met throughout the period April 1, 2019 to March 31, 2020.

Control environment elements

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for other components of internal control, providing discipline and structure. In addition to the tests of design, implementation, and operating effectiveness of controls identified by Microsoft, our procedures included tests of the following relevant elements of Microsoft's control environment:

1. Integrity and Ethical Values
2. Microsoft Standards of Business Conduct
3. Training and Accountability
4. Commitment to Competence
5. Office of Legal Compliance, Internal Audit, Audit Committee
6. Risk Assessment
7. Monitoring
8. Information and Communication

Such tests included inquiry of the appropriate management, supervisory, and staff personnel; observation of Microsoft's activities and operations, inspection of Microsoft's documents and records, and re-performance of the application of Microsoft's controls. The results of these tests were considered in planning the nature, timing, and extent of our testing of the control activities described in this section.

Controls within the control environment have been categorized into the following domains:

1. Information Security (IS)
2. Operator Access (OA)
3. Data Security (DS)
4. Change Management (CM)
5. Secure Development Lifecycle (SDL)
6. Vulnerability Management (VM)
7. Incident Management (IM)
8. Physical and Environmental Security (PE)
9. Logical Access (LA)
10. Business Continuity (BC)
11. Processing Integrity (PI)
12. Additional SOC Controls (SOC2)

13. Additional CCM Controls (CCM)

14. Additional Edge Sites Logical Access Controls (ED)

15. C5 Controls (C5)

Tests of operating effectiveness

Our tests of the controls were designed to cover a representative number of transactions throughout the period from April 1, 2019 to March 31, 2020. 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 nature of the trust services criteria, the CCM criteria, and the objectives set forth in C5 to be achieved, (d) the assessed level of control risk, (e) the expected efficiency and effectiveness of the tests, and (f) the results of our tests of the control environment.

Testing the accuracy and completeness of information provided by Microsoft is also a component of the testing procedures performed. Information we utilized as evidence may have included, but was not limited to:

- Standard "out of the box" reports as configured within the system
- Parameter-driven reports generated by Microsoft's systems
- Custom-developed reports that are not standard to the application such as scripts, report writers, and queries
- Spreadsheets that include relevant information utilized for the performance or testing of a control
- Analysis, schedules, or other evidence manually prepared and utilized by Microsoft

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 Microsoft.

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, 2019 to March 31, 2020. Our tests of controls were performed on controls as they existed during the period of April 1, 2019 to March 31, 2020 and were applied to those controls relating to in-scope trust services criteria, the CCM criteria and the objectives set forth in C5.

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 multiple times throughout 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.

Test	Description
Re-performance of monitoring activities or manual controls	Obtained documents used in the monitoring activity or manual control activity and independently re-performed the procedures. Compared any exception items identified with those identified by the responsible control owner.
Re-performance of programmed processing	Input test data, manually calculated expected results, and compared actual results of processing to expectations.

Reporting on results of testing

The concept of materiality is not applied when reporting the results of tests of controls for which deviations have been identified because Deloitte & Touche LLP does not have the ability to determine whether a deviation will be relevant to a particular user entity. Consequently, Deloitte & Touche LLP reports all deviations.

Results of Testing Performed

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

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

Part B: Contains the CCM Criteria, the related Azure control activities that cover those criteria, and the results of the test procedures performed.

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

Part D: Contains the details of the test procedures performed to test the operating effectiveness of the Azure control activities, and the results of the testing performed.

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

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 Office of Legal Compliance (OLC) 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. OLC 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 Office of Legal Compliance (OLC) 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. OLC 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 assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management.	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. **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 Office of Legal Compliance (OLC) 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. OLC 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 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. **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 Microsoft Online Services Terms, 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	

Trust Criteria	Azure Activity	Test Result
	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 Office of Legal Compliance (OLC) 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. OLC 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. **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.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	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. **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 Microsoft Online Services Terms, 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.	

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. **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.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	SOC2 - 7. Azure maintains and communicates the confidentiality and related security obligations for customer data via the Microsoft Trust Center. **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 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.	

Trust Criteria	Azure Activity	Test Result
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. **BC - 5.** Risk assessments are conducted to identify and assess business continuity risks related to Azure services. **BC - 7.** Datacenter Business Continuity Management (BCM) program to respond to Microsoft's Enterprise Business Continuance Initiative has been implemented and includes documented procedures for performing a Business Impact Analysis, establishing Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), 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 a major disruptive events. **BC - 8.** 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	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	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 - 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 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.,	

Trust Criteria	Azure Activity	Test Result
	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.	
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. **SOC2 - 2.** Azure services maintain an inventory of key information assets. Procedures to review the inventory on a monthly basis are established. **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.	No exceptions noted.

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.** Datacenter Business Continuity Management (BCM) program to respond to Microsoft's Enterprise Business Continuance Initiative has been implemented and includes documented procedures for performing a Business Impact Analysis, establishing Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), 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 a major disruptive events. **BC - 8.** 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 - 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. **VM - 6.** Procedures to monitor the Azure platform components for known security vulnerabilities have been established. Identified security vulnerabilities are remediated.	

Trust Criteria	Azure Activity	Test Result
	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.	
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 - 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.	

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	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	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 - 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. **VM - 6.** Procedures to monitor the Azure platform components for known security vulnerabilities have been established. Identified security vulnerabilities are remediated.	

Trust Criteria	Azure Activity	Test Result
	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.	
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 - 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 - 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.

Trust Criteria	Azure Activity	Test Result
	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.	

CONTROL ACTIVITIES

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	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. **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. **CM - 3.** Responsibilities for requesting, approving, and implementing changes to the Azure platform are segregated among designated personnel. **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 - 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	**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.

Trust Criteria	Azure Activity	Test Result
activities over technology to support the achievement of objectives.	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. **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 to automatically disable Active Directory (AD) accounts and manually remove any non-AD accounts upon user's leave date are in place. **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. **OA - 11.** Procedures have been established to disable access to network devices in the scope boundary for terminated users on a timely basis. **OA - 12.** A quarterly review to validate the appropriateness of access to network devices in the scope boundary is performed by FTE managers. **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.	

Trust Criteria	Azure Activity	Test Result
	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 major changes to the Azure platform follow a defined approach based on the Microsoft Secure Development Lifecycle (SDL) methodology. **SDL - 2.** Applicable operational security and internal control requirements are documented and approved for major releases prior to production deployment.	
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 Office of Legal Compliance (OLC) 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. OLC 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 - 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	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	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.	

LOGICAL AND PHYSICAL ACCESS CONTROLS

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.** Hard Disk Drive destruction guidelines for the disposal of Hard Drives have been established.	**Exception noted:** **OA - 15:** Exceptions were identified in the period previous to the current examination period. Evidence related to password rotation was

Trust Criteria	Azure Activity	Test Result
	DS - 11. Offsite backups are tracked and managed to maintain accuracy of the inventory information. **DS - 12.** Offsite backup tape destruction guidelines have been established and destruction certificates for expired backup tapes are retained. **DS - 15.** Customer data is retained and removed per the defined terms within the Microsoft Online Services Terms (OST), 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. **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	not retained and not available for inspection to corroborate that the passwords were changed on a periodic basis. Per inquiry of management, remediation for this control was in progress from April 1, 2019 through June 30, 2019. D&T sampled 26 samples subsequent to June 30, 2019, and no additional exceptions were noted.

Trust Criteria	Azure Activity	Test Result
	customer administrator are required to be validated before a password change is allowed. SSPR does not display user identifiable information during the password reset. Azure Active Directory 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 - 3.** Procedures to automatically disable Active Directory (AD) accounts and manually remove any non-AD accounts upon user's leave date are in place. **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. **OA - 6.** Production domain-level user accounts for domains where passwords are in use are disabled after 90 days of inactivity.	

Trust Criteria	Azure Activity	Test Result
	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 - 11.** Procedures have been established to disable access to network devices in the scope boundary for terminated users on a timely basis. **OA - 12.** A quarterly review to validate the appropriateness of access to network devices in the scope boundary is performed by FTE managers. **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. **OA - 18.** Azure network is segregated to separate customer traffic from management traffic. **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.	

Trust Criteria	Azure Activity	Test Result
	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 inventory of key information assets. Procedures to review the inventory on a monthly basis are established.	
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. Azure Active Directory 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 - 3.** Procedures to automatically disable Active Directory (AD) accounts and manually remove any non-AD accounts upon user's leave date are in place. **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 for domains where passwords are in use are disabled after 90 days of inactivity.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	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 - 11.** Procedures have been established to disable access to network devices in the scope boundary for terminated users on a timely basis. **OA - 12.** A quarterly review to validate the appropriateness of access to network devices in the scope boundary is performed by FTE managers. **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. Azure Active Directory 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.	**Exception noted:** **OA - 15:** Exceptions were identified in the period previous to the current examination period. Evidence related to password rotation was not retained and not available for inspection to corroborate that the passwords were changed on a periodic basis. Per inquiry of management, remediation for this control was in progress

Trust Criteria	Azure Activity	Test Result
	OA - 3. Procedures to automatically disable Active Directory (AD) accounts and manually remove any non-AD accounts upon user's leave date are in place. **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 for domains where passwords are in use 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 - 11.** Procedures have been established to disable access to network devices in the scope boundary for terminated users on a timely basis. **OA - 12.** A quarterly review to validate the appropriateness of access to network devices in the scope boundary is performed by FTE managers. **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.	from April 1, 2019 through June 30, 2019. D&T sampled 26 samples subsequent to June 30, 2019, and no additional exceptions were noted.

Trust Criteria	Azure Activity	Test Result
CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	**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.	**Exception Noted:** **PE - 3:** For 1 of the 6 sampled datacenter user access reviews from the portion of the period, April 1, 2019 through December 31, 2019, an incomplete listing of access was reviewed during the performance of the control. D&T sampled 10 datacenter user access reviews subsequent to December 31, 2019, and no additional exceptions were noted.
CC6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	**DS - 10.** Hard Disk Drive destruction guidelines for the disposal of Hard Drives have been established. **DS - 12.** Offsite backup tape destruction guidelines have been established and destruction certificates for expired backup tapes are retained. **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.	**Exception Noted:** **PE - 3:** For 1 of the 6 sampled datacenter user access reviews from the portion of the period, April 1, 2019 through December 31, 2019, an incomplete listing of access was reviewed during the performance of the control.

Trust Criteria	Azure Activity	Test Result
	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.	D&T sampled 10 datacenter user access reviews subsequent to December 31, 2019, and no additional exceptions were noted.
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. Keys must have identifiable owners (binding keys to identities) and key management policies. **DS - 10.** Hard Disk Drive destruction guidelines for the disposal of Hard Drives 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.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	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 - 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. Azure Active Directory 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.	

Trust Criteria	Azure Activity	Test Result
	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. **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. Keys must have identifiable owners (binding keys to identities) and key management policies. **DS - 10.** Hard Disk Drive destruction guidelines for the disposal of Hard Drives have been established. **DS - 12.** Offsite backup tape destruction guidelines have been established and destruction certificates for expired backup tapes are retained. **DS - 13.** Production data on backup media is encrypted.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	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.	
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 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. **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.	No exceptions noted.

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. **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.	

Trust Criteria	Azure Activity	Test Result
	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 - 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 (e.g., IPAK team). **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	No exceptions noted.

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 - 13.** Vulnerabilities for network devices are evaluated and mitigated based on documented procedures.	
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to	**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. **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.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
determine whether they represent security events.	**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. **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 - 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 - 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.	
CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	**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.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	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.	
	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.	

Trust Criteria	Azure Activity	Test Result
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 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	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	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.** 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. **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.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	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) 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	

Trust Criteria	Azure Activity	Test Result
	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 to the Azure platform have been documented and communicated. **CM - 2.** Key stakeholders approve changes prior to release into production based on documented change management procedures. **CM - 3.** Responsibilities for requesting, approving, and implementing changes to the Azure platform are segregated among designated personnel. **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. **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 (e.g., IPAK team).	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	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 - 11.** Change management processes include established workflows and procedures to address emergency change requests. **DS - 4.** Cryptographic controls are used for information protection within the Azure platform based on the Azure Cryptographic Policy and Key Management procedures. 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. **SDL - 1.** Development of new features and major changes to the Azure platform follow a defined approach based on the Microsoft Secure Development Lifecycle (SDL) methodology. **SDL - 2.** Applicable operational security and internal control requirements are documented and approved for major releases prior to production deployment. **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.	

Trust Criteria	Azure Activity	Test Result
	SDL - 5. A centralized repository for managing source code changes to the Azure platform is used. Procedures to authorize Azure personnel to submit source code changes based on their role, are established. **SDL - 6.** Source code builds are scanned for malware prior to release to production. **SDL - 7.** The SDL review for each service with a major release is performed and completed on a semi-annual basis, and signed off on by designated owners. **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 inventory of key information assets. Procedures to review the inventory on a monthly basis are established. **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 - 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. **VM - 5.** Procedures to evaluate and implement Microsoft-released patches to Service components have been established.	

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

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. **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.

Trust Criteria	Azure Activity	Test Result
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. **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.	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.** Datacenter Business Continuity Management (BCM) program to respond to Microsoft's Enterprise Business Continuance Initiative has been implemented and includes documented procedures for performing a Business Impact Analysis, establishing Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), mapping processes to pre-defined enterprise functions, establishing	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	recovery strategies as well as developing and conducting test scenarios that enable the BCM program to mitigate risks and vulnerabilities and respond to a major disruptive events. **BC - 8.** 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. **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	**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	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
back-up processes, and recovery infrastructure to meet its objectives.	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. **BC - 7.** Datacenter Business Continuity Management (BCM) program to respond to Microsoft's Enterprise Business Continuance Initiative has been implemented and includes documented procedures for performing a Business Impact Analysis, establishing Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), 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 a major disruptive events. **BC - 8.** 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. **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.	

Trust Criteria	Azure Activity	Test Result
	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.** Offsite backups are tracked and managed to maintain accuracy of the inventory information. **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 Microsoft Online Services Terms (OST), 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.	
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.** Datacenter Business Continuity Management Program defines business continuity planning and testing requirements for functions within the	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	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.	

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.** Hard Disk Drive destruction guidelines for the disposal of Hard Drives have been established. **DS - 12.** Offsite backup tape destruction guidelines have been established and destruction certificates for expired backup tapes are retained. **DS - 15.** Customer data is retained and removed per the defined terms within the Microsoft Online Services Terms (OST), 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.
C1.2. The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	**DS - 10.** Hard Disk Drive destruction guidelines for the disposal of Hard Drives have been established.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	DS - 12. Offsite backup tape destruction guidelines have been established and destruction certificates for expired backup tapes are retained. **DS - 15.** Customer data is retained and removed per the defined terms within the Microsoft Online Services Terms (OST), when a customer's subscription expires, or is terminated.	

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 Microsoft Online Services Terms (OST), 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. **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 Microsoft Online Services 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 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.	No exceptions noted.

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. Azure Active Directory 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 - 12. A quarterly review to validate the appropriateness of access to network devices in the scope boundary is performed by FTE managers. **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 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 - 16.** Each Online Service's customer's data is segregated from other Online Services' customers' data, either logically or physically.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	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.** Hard Disk Drive destruction guidelines for the disposal of Hard Drives have been established. **DS - 12.** Offsite backup tape destruction guidelines have been established and destruction certificates for expired backup tapes are retained. **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 Microsoft Online Services Terms (OST), when a customer's subscription expires, or is terminated.	No exceptions noted.

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

AIS: Application & Interface Security, Application Security

CCM Criteria	Azure Activity	Test Result
AIS-01 Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	**DS - 4.** Cryptographic controls are used for information protection within the Azure platform based on the Azure Cryptographic Policy and Key Management procedures. Keys must have identifiable owners (binding keys to identities) and key management policies. **SDL - 1.** Development of new features and major changes to the Azure platform follow a defined approach based on the Microsoft Secure Development Lifecycle (SDL) methodology. **SDL - 2.** Applicable operational security and internal control requirements are documented and approved for major releases prior to production deployment. **SDL - 7.** The SDL review for each service with a major release is performed and completed on a semi-annual basis, and signed off on by designated owners.	No exceptions noted.
AIS-02 Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	**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. **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 Microsoft Online Services Terms, Microsoft Online Subscription Agreement, Azure service Privacy Statement and Technical Overview of the Security Features in Azure service.	No exceptions noted.
AIS-03 Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	**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.

CCM Criteria	Azure Activity	Test Result
AIS-04 Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity and availability) across multiple system interfaces, jurisdictions and business functions to prevent improper disclosure, alteration, or destruction.	**DS - 4.** Cryptographic controls are used for information protection within the Azure platform based on the Azure Cryptographic Policy and Key Management procedures. 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.	No exceptions noted.

AAC: Audit Assurance & Compliance, Audit Planning

CCM Criteria	Azure Activity	Test Result
AAC-01 Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.	**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.
AAC-02 Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.	**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.

CCM Criteria	Azure Activity	Test Result
AAC-03 Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.	**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.

BCR: Business Continuity Management & Operational Resilience, Business Continuity Planning

CCM Criteria	Azure Activity	Test Result
BCR-01 A consistent unified framework for business continuity planning and plan development shall be established, documented and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update, and approval	**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 for different loss scenario. Each loss scenario is tested at least annually. Issues identified during testing are resolved and plans are updated accordingly. **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.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
• Defined lines of communication, roles, and responsibilities • Detailed recovery procedures, manual work-around, and reference information • Method for plan invocation		
BCR-02 Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.	**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.	No exceptions noted.
BCR-03 Datacenter utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.	**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. **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.
BCR-04 Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following:	**SOC2 - 8.** Azure maintains and distributes an accurate system description to authorized users.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
• Configuring, installing, and operating the information system • Effectively using the system's security features		
BCR-05 Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.	**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. **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.
BCR-06 To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.	**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.	No exceptions noted.
BCR-07 Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.	**PE - 6.** Datacenter Management team maintains and tests datacenter-managed environmental equipment within the facility according to documented policy and maintenance procedures.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
BCR-08 Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific Business Impact Assessment.	**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 - 5.** Risk assessments are conducted to identify and assess business continuity risks related to Azure services.	No exceptions noted.
BCR-09 There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following: • Identify critical products and services • Identify all dependencies, including processes, applications, business partners, and third party service providers • Understand threats to critical products and services • Determine impacts resulting from planned or unplanned disruptions and how these vary over time • Establish the maximum tolerable period for disruption • Establish priorities for recovery • Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption • Estimate the resources required for resumption	**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 for different loss scenario. Each loss scenario is tested at least annually. Issues identified during testing are resolved and plans are updated accordingly. **BC - 5.** Risk assessments are conducted to identify and assess business continuity risks related to Azure services.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
BCR-10 Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery and support of the organization's IT capabilities supporting business functions, workforce, and / or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular workforce training.	**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. **CM - 1.** Procedures for managing different types of changes to the Azure platform have been documented and communicated. **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. **IS - 1.** A security policy that defines the information security rules and requirements for the Service environment 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.	No exceptions noted.
BCR-11 Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.	**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. **DS - 15.** Customer data is retained and removed per the defined terms within the Microsoft Online Services Terms (OST), when a customer's subscription expires, or is terminated.	No exceptions noted.

CCC: Change Control & Configuration Management, New Development / Acquisition

CCM Criteria	Azure Activity	Test Result
CCC-01 Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and / or acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate, operations and / or datacenter facilities have been pre-authorized by the organization's business leadership or other accountable business role or function.	**CM - 1.** Procedures for managing different types of changes to the Azure platform have been documented and communicated. **SDL - 1.** Development of new features and major changes to the Azure platform follow a defined approach based on the Microsoft Secure Development Lifecycle (SDL) methodology.	No exceptions noted.
CCC-02 External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g., ITIL service management processes).	**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.	No exceptions noted.
CCC-03 Organization shall follow a defined quality change control and testing process (e.g., ITIL Service Management) with established baselines, testing, and release standards that focus on system availability, confidentiality, and integrity of systems and services.	**CM - 1.** Procedures for managing different types of changes to the Azure platform have been documented and communicated. **CM - 2.** Key stakeholders approve changes prior to 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. **SOC2 - 15.** Azure has established baselines for OS deployments.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
	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.	
CCC-04 Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	**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. **PE - 1.** Procedures to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors, have been established. **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. **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.	No exceptions noted.
CCC-05 Policies and procedures shall be established for managing the risks associated with applying changes to: • Business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations.	**CM - 1.** Procedures for managing different types of changes to the Azure platform have been documented and communicated. **CM - 2.** Key stakeholders approve changes prior to 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.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
• Infrastructure network and systems components. Technical measures shall be implemented to provide assurance that all changes directly correspond to a registered change request, business-critical or customer (tenant), and / or authorization by, the customer (tenant) as per agreement (SLA) prior to deployment.	**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.	

DSI: Data Security & Information Lifecycle Management, Classification

CCM Criteria	Azure Activity	Test Result
DSI-01 Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.	**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.	No exceptions noted.
DSI-02 Policies and procedures shall be established, and supporting business processes and technical measures implemented, to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's geographically distributed (physical and virtual) applications and infrastructure network and systems components and / or shared with other third parties to ascertain any regulatory, statutory, or supply chain agreement (SLA) compliance impact, and to address any other business risks associated	**SOC2 - 2.** Azure services maintain an inventory of key information assets. Procedures to review the inventory on a monthly basis are established. **SOC2 - 7.** Azure maintains and communicates the confidentiality and related security obligations for customer data via the Microsoft Trust Center. **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.

CCM Criteria	Azure Activity	Test Result
with the data. Upon request, provider shall inform customer (tenant) of compliance impact and risk, especially if customer data is used as part of the services.	**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 - 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.	
DSI-03 Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data.	**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. **OA - 16.** Network filtering to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted service components is implemented.	No exceptions noted.
DSI-04 Policies and procedures shall be established for the labeling, handling, and security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.	**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 inventory of key information assets. Procedures to review the inventory on a monthly basis are established.	No exceptions noted.
DSI-05 Production data shall not be replicated or used in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory	**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.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
requirements for scrubbing of sensitive data elements.		
DSI-06 All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.	**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 inventory of key information assets. Procedures to review the inventory on a monthly basis are established.	No exceptions noted.
DSI-07 Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.	**DS - 10.** Hard Disk Drive destruction guidelines for the disposal of Hard Drives have been established. **DS - 12.** Offsite backup tape destruction guidelines have been established and destruction certificates for expired backup tapes are retained.	No exceptions noted.

DCS: Datacenter Security, Asset Management

CCM Criteria	Azure Activity	Test Result
DCS-01 Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and / or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership by defined roles and responsibilities.	**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 inventory of key information assets. Procedures to review the inventory on a monthly basis are 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	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
	authorized by system owners. System components / assets are tracked in the GDCO ticketing database.	
DCS-02 Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.	**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.	No exceptions noted.
DCS-03 Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.	**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. **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 - 9.** User groups and Access Control Lists have been established to restrict access to network devices in the scope boundary. **OA - 14.** Access to network devices in the scope boundary requires two-factor authentication and / or other secure mechanisms.	No exceptions noted.
DCS-04 Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.	**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 - 12.** Offsite backup tape destruction guidelines have been established and destruction certificates for expired backup tapes are retained.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
DCS-05 Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premises. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full overwrite of the drive to ensure that the erased drive is released to inventory for reuse and deployment, or securely stored until it can be destroyed.	**DS - 10.** Hard Disk Drive destruction guidelines for the disposal of Hard Drives have been established. **DS - 12.** Offsite backup tape destruction guidelines have been established and destruction certificates for expired backup tapes are retained.	No exceptions noted.
DCS-06 Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information.	**PE - 1.** Procedures to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors, have been established. **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.	**Exception Noted:** **PE - 3:** For 1 of the 6 sampled datacenter user access reviews from the portion of the period, April 1, 2019 through December 31, 2019, an incomplete listing of access was reviewed during the performance of the control. D&T sampled 10 datacenter user access reviews subsequent to December 31, 2019, and no additional exceptions were noted.

CCM Criteria	Azure Activity	Test Result
DCS-07 Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.	**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 - 5.** The datacenter facility is monitored 24x7 by security personnel.	No exceptions noted.
DCS-08 Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.	**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.	No exceptions noted.
DCS-09 Physical access to information assets and functions by users and support personnel shall be restricted.	**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 - 5.** The datacenter facility is monitored 24x7 by security personnel.	No exceptions noted.

EKM: Encryption & Key Management, Entitlement

CCM Criteria	Azure Activity	Test Result
EKM-01 Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.	**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. Keys must have identifiable owners (binding keys to identities) and key management policies.	No exceptions noted.
EKM-02 Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and / or the customer (tenant) has some shared responsibility over implementation of the control.	**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. Keys must have identifiable owners (binding keys to identities) and key management policies.	No exceptions noted.
EKM-03 Policies and procedures shall be established, and supporting business processes and technical measures	**DS - 2.** Customer data communicated through Azure service interfaces is encrypted during transmission over external networks.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.	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 - 13.** Production data on backup media is encrypted. **LA - 4.** Customer data that is designated as "confidential" is protected while in storage within Azure services. **ED - 1.** Production servers that resides in edge locations are encrypted at the drive level.	
EKM-04 Platform and data-appropriate encryption (e.g., AES-256) in open / validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.	**DS - 4.** Cryptographic controls are used for information protection within the Azure platform based on the Azure Cryptographic Policy and Key Management procedures. Keys must have identifiable owners (binding keys to identities) and key management policies.	No exceptions noted.

GRM: Governance and Risk Management, Baseline Requirements

CCM Criteria	Azure Activity	Test Result
GRM-01 Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable	**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	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
legal, statutory and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and authorized based on business need.	environment. The Azure OS and component teams review and update configuration settings and baseline configurations at least annually.	
GRM-02 Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following: • Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure • Compliance with defined retention periods and end-of-life disposal requirements • Data classification and protection from unauthorized use, access, loss, destruction, and falsification	**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.	No exceptions noted.
GRM-03 Managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and	**IS - 3.** Management has established defined roles and responsibilities to oversee implementation of the Security Policy across Azure.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
standards that are relevant to their area of responsibility.	**IS - 4.** An information security education and awareness program that includes policy training and periodic security updates for Azure personnel has been established.	
GRM-04 An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business: • Risk management • Security policy • Organization of information security • Asset management • Human resources security • Physical and environmental security • Communications and operations management • Access control • Information systems acquisition, development, and maintenance	**IS - 1.** A security policy that defines the information security rules and requirements for the Service environment has been established and communicated. **PE - 1.** Procedures to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors, have been established. **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.
GRM-05 Executive and line management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has been assigned.	**IS - 3.** Management has established defined roles and responsibilities to oversee implementation of the Security Policy across Azure. **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.

CCM 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.	
GRM-06 Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.	**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.	No exceptions noted.
GRM-07 A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures.	**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.
GRM-08 Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.	**IS - 2.** The Security Policy is reviewed and approved annually by appropriate 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	No exceptions noted.

CCM 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.	
GRM-09 The organization's business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.	**IS - 2.** The Security Policy is reviewed and approved annually by appropriate management.	No exceptions noted.
GRM-10 Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit	**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	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
results, threat and vulnerability analysis, and regulatory compliance).	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.	
GRM-11 Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and stakeholder 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.	No exceptions noted.

HRS: Human Resources, Asset Returns

CCM Criteria	Azure Activity	Test Result
HRS-01 Upon termination of workforce personnel and / or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period.	**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.
HRS-02 Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and	**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.

CCM Criteria	Azure Activity	Test Result
third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.	being granted access. Additional screening is conducted in accordance with customer specific requirements, for employees with access to applicable data.	
HRS-03 Employment agreements shall incorporate provisions and / or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.	**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.
HRS-04 Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, 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.	No exceptions noted.
HRS-05 Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring).	**CCM - 1.** Microsoft Azure has established policies for mobile computing devices to meet appropriate security practices prior to being connected to the production environment. **IS - 4.** An information security education and awareness program that includes policy training and periodic security updates for Azure personnel has been established.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
HRS-06 Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals.	**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.
HRS-07 Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.	**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.
HRS-08 Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to corporate resources (i.e., BYOD) shall be considered and incorporated as appropriate.	**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.	No exceptions noted.
HRS-09 A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access	**IS - 4.** An information security education and awareness program that includes policy training and periodic security updates for Azure personnel has been established.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.		
HRS-10 All personnel shall be made aware of their roles and responsibilities for: • Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations. • Maintaining a safe and secure working environment	**IS - 3.** Management has established defined roles and responsibilities to oversee implementation of the Security Policy across Azure. **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.
HRS-11 Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions are disabled after an established period of inactivity.	**CCM - 2.** Microsoft Azure has included a clear desk and clear screen policy which users are provided as a part of onboarding.	No exceptions noted.

IAM: Identity & Access Management, Audit Tools Access

CCM Criteria	Azure Activity	Test Result
IAM-01 Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segregated and access restricted to prevent	**CCM - 3.** 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.

CCM Criteria	Azure Activity	Test Result
inappropriate disclosure and tampering of log data.		
IAM-02 User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following: • Procedures and supporting roles and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships) • Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems)	**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. **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 - 3.** Logical segregation to restrict unauthorized access to other customer tenants is implemented. **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 - 8.** Authentication over an encrypted Remote Desktop Connection is used for administrator access to the production environment. **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.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
• Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and / or other customer (tenant)) • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation) • Account credential lifecycle management from instantiation through revocation • Account credential and / or identity store minimization or re-use when feasible • Authentication, authorization, and accounting (AAA) rules for access to data and sessions (e.g., encryption and strong / multi-factor, expireable, non-shared authentication secrets) • Permissions and supporting capabilities for customer (tenant) controls over authentication, authorization, and accounting (AAA) rules for access to data and sessions • Adherence to applicable legal, statutory, or regulatory compliance requirements		
IAM-03 User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	**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 - 9.** User groups and Access Control Lists have been established to restrict access to network devices in the scope boundary.	No exceptions noted.

CCM 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.	
IAM-04 Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.	**IS - 1.** A security policy that defines the information security rules and requirements for the Service environment 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 - 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.	No exceptions noted.
IAM-05 User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.	**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.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
IAM-06 Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.	**CM - 3.** Responsibilities for requesting, approving, and implementing changes to the Azure platform are segregated among designated personnel. **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. **SDL - 5.** A centralized repository for managing source code changes to the Azure platform is used. Procedures to authorize Azure personnel to submit source code changes based on their role, are established.	No exceptions noted.
IAM-07 The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.	**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.	No exceptions noted.
IAM-08 Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.	**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. **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.
IAM-09 Provisioning user access (e.g., employees, contractors, customers (tenants), business partners and / or supplier	**OA - 1.** Administrative access to the Service environment is controlled through defined interfaces that require authentication using appropriate credentials.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, provider shall inform customer (tenant) of this user access, especially if customer (tenant) data is used as part the service and / or customer (tenant) has some shared responsibility over implementation of control.	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 - 10.** Users are granted access to network devices in the scope boundary upon receiving appropriate approvals. **PE - 1.** Procedures to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors, have been established. **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 - 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.	
IAM-10 User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow established user access policies and procedures.	**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 - 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.

CCM Criteria	Azure Activity	Test Result
IAM-11 Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and / or customer (tenant) has some shared responsibility over implementation of control.	**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 to automatically disable Active Directory (AD) accounts and manually remove any non-AD accounts upon user's leave date are in place. **OA - 6.** Production domain-level user accounts for domains where passwords are in use are disabled after 90 days of inactivity. **OA - 11.** Procedures have been established to disable access to network devices in the scope boundary for terminated users on a timely basis. **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.
IAM-12 Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures: • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation)	**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. **OA - 4.** User credentials adhere to established corporate standards and group policies for password requirements: - expiration - length - complexity - history	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
• Account credential lifecycle management from instantiation through revocation • Account credential and / or identity store minimization or re-use when feasible • Adherence to industry acceptable and / or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong / multi-factor, expirable, non-shared authentication secrets)	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.	
IAM-13 Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.	**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.

IVS: Infrastructure & Virtualization Security, Audit Logging / Intrusion Detection

CCM Criteria	Azure Activity	Test Result
IVS-01 Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and / or file integrity anomalies, and to support	**CCM - 3.** 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.

CCM Criteria	Azure Activity	Test Result
forensic investigative capabilities in the event of a security breach.		
IVS-02 The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g., dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g., portals or alerts).	**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 - 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 - 4.** Procedures to investigate and respond to malicious events detected by the Azure monitoring system in a timely manner have been established. **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.
IVS-03 A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.	**CCM - 4.** Microsoft Azure components are configured to use Coordinated Universal Time (UTC) time and the clocks are synchronized with the domain controller server.	No exceptions noted.
IVS-04 The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in	**BC - 10.** The network is monitored to ensure availability and address capacity issues in a timely manner.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.	**CCM - 5.** Microsoft Capacity Management team projects future capacity requirements based on internal operational reports, revenue forecasts and inputs from internal component teams. **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. **VM - 12.** The availability of Azure services is monitored through third-party and internal tools, and the status is communicated through a Service Dashboard.	
IVS-05 Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g., virtualization aware).	**VM - 6.** Procedures to monitor the Azure platform components for known security vulnerabilities have been established. Identified security vulnerabilities are remediated. **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.
IVS-06 Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services,	**OA - 16.** Network filtering to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted service components is implemented. **OA - 18.** Azure network is segregated to separate customer traffic from management traffic. **VM - 1.** Azure platform components are configured to log and collect security events.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
protocols, and ports, and by compensating controls.	**VM - 9.** Network devices in the scope boundary are configured to log and collect security events, and monitored for compliance with established security standards.	
IVS-07 Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.	**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. **ED - 3.** All unused IO ports on production servers that reside in edge locations are disabled through the configuration settings at the OS-level.	No exceptions noted.
IVS-08 Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain / realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.	**CM - 3.** Responsibilities for requesting, approving, and implementing changes to the Azure platform are segregated among designated personnel. **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.	No exceptions noted.
IVS-09 Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations:	**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.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
• Established policies and procedures • Isolation of business critical assets and / or sensitive user data, and sessions that mandate stronger internal controls and high levels of assurance • Compliance with legal, statutory and regulatory compliance obligations		
IVS-10 Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from production-level networks for such migrations.	**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. Keys must have identifiable owners (binding keys to identities) and key management policies. **OA - 18.** Azure network is segregated to separate customer traffic from management traffic.	No exceptions noted.
IVS-11 Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).	**DS - 3.** Internal communication between key Azure components where customer data is transmitted / involved is secured using encryption. **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 - 16.** Network filtering to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted service components is implemented. **VM - 2.** Administrator activity in the Azure platform is logged.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
IVS-12 Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following: • Perimeter firewalls implemented and configured to restrict unauthorized traffic • Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings) • User access to wireless network devices restricted to authorized personnel • The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network	**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. **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. **VM - 9.** Network devices in the scope boundary are configured to log and collect security events, and monitored for compliance with established security standards.	No exceptions noted.
IVS-13 Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and / or distributed denial-of-service (DDoS) attacks.	**OA - 16.** Network filtering to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted service components is implemented. **SDL - 1.** Development of new features and major changes to the Azure platform follow a defined approach based on the Microsoft Secure Development Lifecycle (SDL) methodology. **SDL - 2.** Applicable operational security and internal control requirements are documented and approved for major releases prior to production deployment. **SOC2 - 8.** Azure maintains and distributes an accurate system description to authorized users. **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.

CCM Criteria	Azure Activity	Test Result
	VM - 9. Network devices in the scope boundary are configured to log and collect security events, and monitored for compliance with established security standards.	

IPY: Interoperability & Portability, APIs

CCM Criteria	Azure Activity	Test Result
IPY-01 The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	**CCM - 6.** Azure has published a standard set of APIs with an ecosystem of tools and libraries on the Azure Portal.	No exceptions noted.
IPY-02 All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files)	**SOC2 - 28.** Customer data is accessible within agreed upon services in data formats compatible with providing those services.	No exceptions noted.
IPY-03 Policies, procedures, and mutually-agreed upon provisions and / or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence.	**CCM - 6.** Azure has published a standard set of APIs with an ecosystem of tools and libraries on the Azure Portal.	No exceptions noted.
IPY-04 The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the	**DS - 2.** Customer data communicated through Azure service interfaces is encrypted during transmission over external networks.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.	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. **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. **SOC2 - 8.** Azure maintains and distributes an accurate system description to authorized users.	
IPY-05 The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use and all solution-specific virtualization hooks available for customer review.	**OA - 19.** Microsoft Azure has published virtualization industry standards supported within its environment.	No exceptions noted.

MOS: Mobile Security, Anti-Malware

CCM Criteria	Azure Activity	Test Result
MOS Criteria - Not Applicable as Microsoft Azure does not support mobile devices		

SEF: Security Incident Management, E-Discovery & Cloud Forensics, Contact / Authority Maintenance

CCM Criteria	Azure Activity	Test Result
SEF-01 Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and / or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.	**IM - 4.** Incident post-mortem activities for severe incidents impacting the Azure environment are conducted. **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. **CCM - 9.** Microsoft Azure has established forensic procedures to support potential legal action after an information security incident.	No exceptions noted.
SEF-02 Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.	**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.
SEF-03 Workforce personnel and external business relationships shall be informed of their responsibilities and, if required, shall consent and / or contractually agree to report all information security events in a timely manner. Information security events	**IS - 3.** Management has established defined roles and responsibilities to oversee implementation of the Security Policy across Azure. **SOC2 - 6.** Azure maintains a Customer Support website that describes the process for customers and other external users to inform about potential	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.	security issues and submit complaints. Reported issues are reviewed and addressed per documented incident management procedures. **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.	
SEF-04 Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and / or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.	**CCM - 9.** Microsoft Azure has established forensic procedures to support potential legal action after an information security incident. **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. **IM - 4.** Incident post-mortem activities for severe incidents impacting the Azure environment are conducted.	No exceptions noted.
SEF-05 Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.	**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.

STA: Supply Chain Management, Transparency and Accountability, Data Quality and Integrity

CCM Criteria	Azure Activity	Test Result
STA-01 Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.	**CM - 3.** Responsibilities for requesting, approving, and implementing changes to the Azure platform are segregated among designated personnel. **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. **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. **SDL - 3.** Responsibilities for submitting and approving production deployments are segregated within the Azure teams. **SDL - 5.** A centralized repository for managing source code changes to the Azure platform is used. Procedures to authorize Azure personnel to submit source code changes based on their role, are 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.	No exceptions noted.
STA-02 The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals).	**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.

CCM Criteria	Azure Activity	Test Result
STA-03 Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.	**SDL - 1.** Development of new features and major changes to the Azure platform follow a defined approach based on the Microsoft Secure Development Lifecycle (SDL) methodology. **SDL - 2.** Applicable operational security and internal control requirements are documented and approved for major releases prior to production deployment. **SDL - 7.** The SDL review for each service with a major release is performed and completed on a semi-annual basis, and signed off on by designated owners.	No exceptions noted.
STA-04 The provider shall perform annual internal assessments of conformance to, and effectiveness of, its policies, procedures, and supporting measures and metrics.	**IS - 2.** The Security Policy is reviewed and approved annually by appropriate 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.
STA-05 Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and / or terms: • Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems	**SOC2 - 7.** Azure maintains and communicates the confidentiality and related security obligations for customer data via the Microsoft Trust Center. **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 - 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	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations) • Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships • Notification and / or pre-authorization of any changes controlled by the provider with customer (tenant) impacts • Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain) • Assessment and independent verification of compliance with agreement provisions and / or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk	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.	

CCM Criteria	Azure Activity	Test Result
of exposure to the organization being assessed • Expiration of the business relationship and treatment of customer (tenant) data impacted • Customer (tenant) service-to-service application (API) and data interoperability and portability requirements for application development and information exchange, usage, and integrity persistence		
STA-06 Providers shall review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.	**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.	No exceptions noted.
STA-07 Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream / downstream). Reviews shall be performed at least annually and identify any non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.	**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. **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.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
STA-08 Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review shall include all partners / third party-providers upon which their information supply chain depends on.	**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. **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.	No exceptions noted.
STA-09 Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.	**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. **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.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
TVM-01 Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	**SDL - 6.** Source code builds are scanned for malware prior to release to production. **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.
TVM-02 Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and / or customer (tenant) has some shared responsibility over implementation of control.	**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 - 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 - 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. **CM - 7.** Secure network configurations are applied and reviewed through defined change management procedures.	No exceptions noted.

CCM 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 (e.g., IPAK team). **CM - 10.** Secure configurations for datacenter software are applied through defined change management procedures including documentation, testing and approval.	
TVM-03 Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	**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.

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

Framework conditions of the cloud service (surrounding parameters for transparency)

Control Objective 4.1: The general organizational and legal framework conditions and targets are described comprehensibly and accurately for a third party expert in order to assess the general suitability of the cloud service for the desired application.

C5 Requirements	Azure Activity	Test Result
UP-01 In their system description, the cloud provider provides comprehensible and transparent specifications regarding the cloud service, which allow an expert third party to assess the general suitability of the cloud service for the desired application. The system description describes the following aspects: • Type and scope of the cloud services rendered according to the service level agreement which is typically based on a contract concluded with the cloud customers, • Principles, procedures and safeguards for rendering (development and / or operation) the cloud service, including the controls established, • Description of the infrastructure, network and system components used for the development and operation of the cloud service, • Handling of significant incidents and conditions which constitute exceptions to regular operations, such as the failure of critical IT systems,	**D&T Note:** D&T inquired of management regarding the process for developing the system description and the specifications made available to user entities through the Azure website, which include specifications of Azure services, which would allow a third party to assess the general suitability of Azure for the desired application. D&T inspected the system description to ascertain that the system description describes the type and scope of the Azure system; principles, procedures and safeguards; description of the infrastructure, network and system components used for the development and operation of Azure; handling of significant incidents and conditions; and roles and responsibilities of Microsoft, and the cloud customer.	No exceptions noted.

C5 Requirements	Azure Activity	Test Result
• Roles and responsibilities of the cloud provider and the cloud customer, including the duties to cooperate and corresponding controls at the cloud customer, • Functions assigned or outsourced to subcontractors.		
UP-02 In service level agreements, their process documentation or comparable documentation, the cloud provider provides comprehensible and transparent specifications regarding its jurisdiction as well as with respect to data storage, processing and backup locations, which allow an expert third party to assess the general suitability of the cloud service for the customer application. This also holds true if data of the cloud customer is processed, stored and backed up by subcontractors of the cloud provider. Data of the cloud customer shall only be processed, stored and backed up outside the contractually agreed locations only with the prior express written consent of the cloud customer.	**D&T Note:** D&T inquired of management regarding the service level agreement specifications and subscription agreements allowing customers the ability to grant administrator rights to third parties. Additionally, inquired of management regarding cloud customer data processed, stored and backed up outside of Azure SOC boundary. D&T inspected the service level agreement specifications to ascertain that service level agreements provide specifications regarding their jurisdiction as well as with respect to data storage, processing and backup locations. Additionally, ascertained that data of the cloud customer shall be processed, stored and backed up within Azure SOC boundary. D&T inspected the subscription agreement and ascertained that it addressed customers' ability to grant administrator rights to third parties.	No exceptions noted.
UP-03 In service level agreements, their process documentation or comparable documentation, the cloud provider provides comprehensible and transparent specifications regarding applicable disclosure and investigatory powers of government agencies which allow access to data of the	**D&T Note:** D&T inquired of management regarding the service level agreement specifications for disclosure and investigatory powers of government agencies and subscription agreements allowing customers the ability to grant administrator rights to third parties.	No exceptions noted.

C5 Requirements	Azure Activity	Test Result
cloud customer. The specifications must allow an expert third party to assess the general suitability of the cloud service for the customer application. If the cloud provider accesses third-party services, the provider has obtained these specifications from them.	D&T inspected the service level agreement specifications to ascertain that service level agreements provide specifications regarding disclosure of customer data including to government agencies. D&T inspected the subscription agreement and ascertained that it addressed customers' ability to grant administrator rights to third parties.	
UP-04 In service level agreements, their process documentation or comparable documentation, the cloud provider provides comprehensible and transparent specifications regarding available and valid certifications and certificates of independent third parties, which allow an expert third party to assess the general suitability of the cloud service for the customer application.	**D&T Note:** D&T inquired of management regarding their disclosure to customers of available and valid certifications and certificates of independent third parties. D&T inspected the Microsoft Trust Center website and ascertained that available and valid certifications and certificates of independent third parties are disclosed.	No exceptions noted.

OIS: Organization of Information Security

Control Objective 5.1: Planning, implementation, maintenance and continuous improvement of a framework regarding information security within the organization.

C5 Requirements	Azure Activity	Test Result
OIS-01 The top management initiates, controls and monitors an information security management system (ISMS) which is based on ISO standards of the 2700x series.	**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 Requirements	Azure Activity	Test Result
• The instruments and methods used allow a comprehensible control of the following tasks and activities to permanently maintain and ensure information security: Planning, implementing the plan and / or carrying out the project, • Performance review and / or monitoring the achievement of objectives • Eliminating discovered flaws and weaknesses and continuous improvement. The ISMS also includes the IT processes for the development and operation of the cloud service.	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.	
OIS-02 A security policy with security objectives and strategic parameters for achieving these objectives is documented. The security objectives are 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. The strategic targets constitute essential framework conditions which in further policies and instructions are specified in more detail (see SA-01). The security policy is adopted by the top management and communicated to all concerned internal and external parties of the cloud provider (e.g., cloud customers, subcontractors).	**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.	No exceptions noted.

C5 Requirements	Azure Activity	Test Result
OIS-03 Responsibilities shared between the cloud provider and cloud customers, duties to cooperate as well as interfaces for the reporting of security incidents and malfunctions are defined, documented, assigned depending on the respective cloud model (infrastructure, platform or software as a service) and the contractual duties and communicated to all concerned internal and external parties (e.g., cloud customers, subcontractors of the cloud provider). On the part of the cloud provider, at least the following roles (or comparable equivalents) are described in the security policy or associated policies and corresponding responsibilities assigned: • Head of IT (CIO) • IT Security Officer (CISO) • Representative for the handling of IT security incidents (e.g., Head of CERT) Changes to the responsibilities and interfaces are communicated internally and externally in such a timely manner that all internal and external parties concerned (e.g., cloud customers) are able to respond to them appropriately with organizational and technical safeguards, before the change becomes effective.	**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. **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 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.
OIS-04 Organizational and technical controls are established in order to ensure the separation of roles and responsibilities (also	**SOC2 - 18.** Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements for each information system	No exceptions noted.

C5 Requirements	Azure Activity	Test Result
referred to the "separation of duties") which are incompatible with respect to the confidentiality, integrity and availability of information of the cloud customers. Controls for the separation of functions are established in the following areas in particular: • Administration of roles, granting and assignment of access authorizations for users under the responsibility of the cloud provider, • Development and implementation of changes to the cloud service, • Maintenance of the physical and logical IT infrastructure relevant to the cloud service (networks, operating systems, databases) and the IT applications if they are in the cloud provider's area of responsibility according to the contractual agreements with the cloud customers. Operative and controlling functions should not be performed by one and the same person at the same time. If it is not possible to achieve a separation of duties for organizational or technical reasons, appropriate compensating controls are established in order to prevent or uncover improper activities.	and the organization, should be explicitly defined, documented, and kept up to date. **CM - 3.** Responsibilities for requesting, approving, and implementing changes to the Azure platform are segregated among designated personnel. **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.	
OIS-05 Appropriate and relevant contacts of the cloud provider with government agencies and interest groups are established to be	**SOC2 - 18.** Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements for each information system	No exceptions noted.

C5 Requirements	Azure Activity	Test Result
always informed about current threat scenarios and countermeasures.	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.	
OIS-06 Policies and instructions for the general procedure applicable to the identification, analysis, assessment and handling of risks and IT risks in particular are documented, communicated and provided according to SA-01.	**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.
OIS-07 The procedures for the identification, analysis, assessment and handling of risks, including the IT risks relevant to the cloud service are done at least once a year in order to take internal and external changes and influencing factors into account. The identified risks are comprehensibly documented, assessed and provided with mitigating safeguards according to the safeguards of the risk management.	**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.

SA: Security Policies and Work Instructions

Control Objective 5.2: Providing policies and instructions with respect to the security claim and to support the business requirements.

C5 Requirements	Azure Activity	Test Result
SA-01 Policies and instructions for information security or related topics derived from the security policy are documented in a uniform structure. They are communicated and made available to all internal and external employees of the cloud provider properly and adequately. Policies are versioned and approved by top management of the cloud provider. The policies and instructions describe at least the following aspects: • Goals • Scopes of application • Roles and responsibilities, including requirements for the qualification of the personnel and the establishment of substitution arrangements, • Coordination of different company departments, • Security architecture and safeguards for the protection of data, IT applications and IT infrastructures which are managed by the cloud provider or third parties as well as • Safeguards for the compliance with legal and regulatory requirements (compliance).	**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. **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.	No exceptions noted.

C5 Requirements	Azure Activity	Test Result
SA-02. The policies and instructions for information security are reviewed with respect to their appropriateness and effectiveness by specialists of the cloud provider who are familiar with the topic at least once a year. At least the following aspects are taken into account in the review: • Organizational changes at the cloud provider, • Current and future expected threat environment regarding information security as well as • Legal and technical changes in the cloud provider's environment. Revised policies and instructions are approved by committees or bodies of the cloud provider authorized to do so before they become valid.	**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 - 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.
SA-03 Exceptions of policies and instructions for information security are approved by committees or bodies of the cloud provider authorized to do so in a documented form. The appropriateness of approved exceptions and the assessment of the risks resulting from this are reviewed by specialists of the cloud provider who are familiar with the topic against the backdrop of the current and future expected threat environment	**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.

C5 Requirements	Azure Activity	Test Result
regarding information security at least once a year.		

HR: Personnel

Control Objective 5.3: Making sure that employees, service providers and suppliers understand their tasks, that they are aware of their responsibility with regard to information security and that the assets of the organization are protected if the tasks are modified or completed.

C5 Requirements	Azure Activity	Test Result
HR-01 The background of all internal and external employees of the cloud provider with access to data of the cloud customers or of the shared IT infrastructure is checked according to the local legislation and regulation by the cloud provider prior to the start of the employment relationship. To the extent permitted by law, the security check includes the following areas: • Verification of the person by means of the identity card, • Verification of the curriculum vitae, • Verification of academic titles and degrees, • Request of a police clearance certificate for sensitive posts in the company	**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.	No exceptions noted.
HR-02 Employment agreements include the obligations of the cloud provider's internal and external employees to comply with relevant laws, regulations and provisions	**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	No exceptions noted.

C5 Requirements	Azure Activity	Test Result
regarding information security (see KOS-10). The security policy as well as the policies and instructions for information security derived from this are added to the employment agreement documents. Corresponding compliance is confirmed by the employee by a written statement before they can access the data of the cloud customers or the (shared) IT infrastructure.	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.	
HR-03 A security training and awareness-raising program tailored to specific target groups on the topic of information security is available and mandatory for all internal and external employees of the cloud provider. The program is updated at regular intervals with respect to the applicable policies and instructions, the assigned roles and responsibilities as well as the known threats and must then be run through again. The program includes at least the following contents: • Regular and documented instruction on the secure configuration and secure operation of the IT applications and IT infrastructure required for the cloud service, including mobile terminal devices, • Appropriate handling of data of the cloud customers, • Regular and documented instruction on known basic threats, and	**IS - 4.** An information security education and awareness program that includes policy training and periodic security updates for Azure personnel has been established.	No exceptions noted.

C5 Requirements	Azure Activity	Test Result
• Regular and documented training on the behavior in case of security-relevant events. • External service providers and suppliers of the cloud provider, who contribute to the development or operation of the cloud service, are obliged by contract to make their employees and subcontractors aware of the specific security requirements of the cloud provider and train their employees generally in the subject of information security.		
HR-04 A process for performing disciplinary measures is implemented and communicated to the employees in order to make the consequences of violations of the applicable policies and instructions as well as legal provisions and laws transparent.	**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.
HR-05 Internal as well as external employees are informed that the obligations to comply with relevant laws, regulations and provisions regarding information security remain valid even if the area of responsibility changes or the employment relationship is terminated.	**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.

AM: Asset Management

Control Objective 5.4: Identifying the organization's own assets and the persons responsible and ensuring an appropriate level of protection.

C5 Requirements	Azure Activity	Test Result
AM-01 The assets (e.g., PCs, peripheral devices, telephones, network components, servers, installation documentation, process instructions, IT applications, tools) used to render the cloud service are identified and inventoried. By means of appropriate processes and safeguards, it is ensured that this inventory remains complete, correct, up-to-date and consistent. A history of the changes to the entries in the inventory is kept in a comprehensible manner. If no effective automatic procedures are established for this, this is ensured by a manual review of the inventory data of the assets which takes place at least once a month.	**SOC2 - 2.** Azure services maintain an inventory of key information assets. Procedures to review the inventory on a monthly basis are established.	No exceptions noted.
AM-02 All inventoried assets are assigned to a person responsible on the part of the cloud provider. The persons responsible of the cloud provider are responsible over the entire life cycle of the assets to ensure that they are inventoried completely and classified correctly.	**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.	No exceptions noted.
AM-03 Policies and instructions with technical and organizational safeguards for the proper handling of assets are documented, communicated and provided according to SA-01 in the respectively current version.	**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.	No exceptions noted.

C5 Requirements	Azure Activity	Test Result
AM-04 All internal and external employees of the cloud provider are obliged to return or irrevocably delete all assets which were handed over to them in relation to the cloud service and / or for which they are responsible as soon as the employment relationship has been terminated.	**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.
AM-05 The cloud provider uses a uniform classification of information and assets which are relevant to the development and rendering of the cloud service.	**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. **D&T Note:** Azure development machines were not included in scope for testing the AM-05 requirement as the development environment is completely isolated from the production environment. The changes developed on the development machines have to go through standard change management procedures of testing, scanning, and approval, prior to deployment on the production environment. Thus, we can conclude that the design is appropriate to meet the C5 objective 5.4.	No exceptions noted.
AM-06 Work instructions and processes for the implemented classification scheme of information and assets are in place in order to ensure the labeling of information as well as the corresponding handling of assets. This only refers to assets which store or process information.	**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.	No exceptions noted.
AM-07 Policies and instructions with technical and organizational safeguards for the secure handling of data media of any	**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.

C5 Requirements	Azure Activity	Test Result
type are documented, communicated and provided according to SA-01. The targets establish a reference to the classification of information (see AM-05). They include the secure use, the secure transport as well as the irrevocable deletion and destruction of data media.	**DS - 10.** Hard Disk Drive destruction guidelines for the disposal of Hard Drives have been established. **DS - 12.** Offsite backup tape destruction guidelines have been established and destruction certificates for expired backup tapes are retained.	
AM-08 Devices, hardware, software or data may only be transferred to external premises after it has been approved by authorized committees or bodies of the cloud provider. The transfer takes place securely according to the type of the assets to be transferred.	**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.** Hard Disk Drive destruction guidelines for the disposal of Hard Drives have been established. **DS - 12.** Offsite backup tape destruction guidelines have been established and destruction certificates for expired backup tapes are retained.	No exceptions noted.

PS: Physical Security

Control Objective 5.5: Preventing unauthorized physical site access and protection against theft, damage, loss and failure of operations.

C5 Requirements	Azure Activity	Test Result
PS-01 The perimeter of premises or buildings which house sensitive or critical information, information systems or other network infrastructure are protected in a physically solid manner and by means of	**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.	No exceptions noted.

C5 Requirements	Azure Activity	Test Result
appropriate security safeguards that conform to the current state of the art.	**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.	
PS-02 Access to the premises or buildings which house sensitive or critical information, information systems or other network infrastructure is secured and monitored by means of physical site access controls in order to avoid unauthorized site access.	**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.	**Exception Noted:** **PE - 3:** For 1 of the 6 sampled datacenter user access reviews from the portion of the period, April 1, 2019 through December 31, 2019, an incomplete listing of access was reviewed during the performance of the control. D&T sampled 10 datacenter user access reviews subsequent to December 31, 2019, and no additional exceptions were noted.
PS-03 Structural, technical and organizational safeguards are taken to protect premises or buildings which house sensitive or critical information, information systems or other network infrastructure against fire, water, earthquakes, explosions, civil disturbances and other forms of natural threats and threats caused by humans.	**PE - 1.** Procedures to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors, have been established. **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 Requirements	Azure Activity	Test Result
At two geo-redundant sites, at least the following safeguards are carried out: Structural safeguards: • Setup of a separate fire zone for the computer center, • Use of fire-resistant materials according to DIN 4102-1 or EN 13501 (period of fire resistance of at least 90 minutes) Technical safeguards: • Sensors to monitor temperature and humidity, • Connecting the building to a fire alarm system with notification of the local fire department, • Early fire detection and extinguishing systems. Organizational safeguards: • Regular fire drills and fire safety inspections to check compliance with fire protection measures.		
PS-04 Precautions against the failure of supply services such as power, cooling or network connections are taken by means of suitable safeguards and redundancies in coordination with safeguards for operational reliability. Power and telecommunication supply lines which transport data or supply information	**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 Requirements	Azure Activity	Test Result
systems must be protected against interception and damage.		
PS-05 Policies and instructions with technical and organizational safeguards are documented, communicated and provided according to SA-01 which describe the maintenance (especially remote maintenance), deletion, updating and re-use of assets in information processing in outsourced premises or by external personnel.	**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.	No exceptions noted.

RB: Safeguards for Regular Operations

Control Objective 5.6: Ensuring proper regular operations including appropriate safeguards for planning and monitoring the capacity, protection against malware, logging and monitoring events as well as handling vulnerabilities, malfunctions and errors.

C5 Requirements	Azure Activity	Test Result
RB-01 The planning of capacities and resources (personnel and IT resources) follows an established procedure in order to avoid capacity bottlenecks. The procedures include forecasts of future capacity requirements in order to identify use trends and master system overload risks.	**BC - 10.** The network is monitored to ensure availability and address capacity issues in a timely manner. **CCM - 5.** Microsoft Capacity Management team projects future capacity requirements based on internal operational reports, revenue forecasts and inputs from internal component teams.	No exceptions noted.
RB-02 Technical and organizational safeguards for the monitoring and provisioning and de-provisioning of cloud services are defined. Thus, the cloud	**BC - 10.** The network is monitored to ensure availability and address capacity issues in a timely manner.	No exceptions noted.

C5 Requirements	Azure Activity	Test Result
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.	**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. **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.	
RB-03 The cloud customer is able to determine the locations (city / country) of the data processing and storage including data backups.	**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.
RB-04 In case of IaaS / PaaS, the cloud customer is able to control and monitor the distribution of the system resources assigned to them for administration / use (e.g., computing capacity or storage capacity) in order to prevent resources from being congested.	**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.
RB-05 The logical and physical IT systems which the cloud provider uses for the development and rendering of the cloud service as well as the network perimeters	**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.

C5 Requirements	Azure Activity	Test Result
which are subject to the cloud provider's area of responsibility are equipped with anti-virus protection and repair programs which allow for a signature- and behavior-based detection and removal of malware. The programs are updated according to the contractual agreements concluded with the manufacturer(s), but at least once a day.	**D&T Note:** Azure development machines were not in scope of the examination performed as the development environment is isolated from the production environment. However, it was tested that the changes developed on the development machines go through standard change management procedures of testing, scanning, and approval, prior to deployment on the production environment. Thus, we can conclude that the design is appropriate to meet the C5 Objective 5.6.	
RB-06 Policies and instructions with technical and organizational safeguards in order to avoid losing data are documented, communicated and provided according to SA-01. They provide reliable procedures for the regular backup (backup as well as snapshots, where applicable) and restoration of data. The scope, frequency and duration of the retention comply with the contractual agreements concluded with the cloud customers as well as the cloud provider's business requirements. Access to the data backed up is limited to authorized personnel. Restoration procedures include control mechanisms that ensure that restorations are carried out only after they have been approved by persons authorized to do so according to the contractual agreements with the cloud customers or the internal policies of the cloud provider.	**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 - 14.** Azure services are configured to automatically restore customer services upon detection of hardware and system failures.	No exceptions noted.

C5 Requirements	Azure Activity	Test Result
	DS - 15. Customer data is retained and removed per the defined terms within the Microsoft Online Services Terms (OST), 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.	
RB-07 The process of backing up data is monitored by means of technical and organizational safeguards. Malfunctions are examined and eliminated promptly by qualified employees in order to ensure compliance with the contractual duties towards the cloud customers or the cloud provider's business requirements with respect to the scope, frequency and duration of the retention.	**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.	No exceptions noted.
RB-08 Backup media and restoration procedures must be tested with dedicated test media by qualified employees at regular intervals. The tests are designed in such a way that the reliability of the backup media and the restoration time can be audited with sufficient certainty. The tests are carried out by qualified employees and the results documented comprehensibly. Any occurring errors are eliminated in a timely manner.	**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.	No exceptions noted.
RB-09 The data to be backed up is transmitted to a remote site (e.g., another	**DS - 2.** Customer data communicated through Azure service interfaces is encrypted during transmission over external networks.	No exceptions noted.

C5 Requirements	Azure Activity	Test Result
datacenter of the cloud provider) or transported to a remote site on backup media. If the backup of the data is transmitted to the remote site via a network, this is carried out in an encrypted form that conforms to the state of the art. The distance to the main site should be large enough to ensure that catastrophes there do not lead to a loss of data at the remote site and, at the same time, short enough to be able to fulfill the contractual duties regarding the restoration times. The safeguards taken to ensure the physical and environment-related security at the remote site corresponds to the level at the main site.	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. **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.	
RB-10 Policies and instructions with technical and organizational safeguards are documented, communicated and provided according to SA-01 in order to log events on all assets which are used for the development or operation of the cloud service and to store them in a central place. The logging includes defined events which may impair the security and availability of the cloud service, including logging the activation, stopping and pausing of different logs. In case of unexpected or unusual	**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. **CCM - 3.** 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 Requirements	Azure Activity	Test Result
events, the logs are checked by authorized personnel due to special events in order to allow for a timely examination of malfunctions and security incidents as well as for the initiation of suitable safeguards.	**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. **D&T Note:** Azure development machines were not in scope of the examination performed as the development environment is isolated from the production environment. However, it was tested that the changes developed on the development machines go through standard change management procedures of testing, scanning, and approval, prior to deployment on the production environment. Thus, we can conclude that the design is appropriate to meet the C5 Objective 5.6.	
RB-11 Policies and instructions with technical and organizational safeguards for the secure handling of meta data (user data) are documented, communicated and provided according to SA-01. The meta data is collected and used only for accounting and billing purposes, for eliminating malfunctions and errors (incident management) as well as for processing security incidents (security incident management). The meta data is not used for commercial purposes.	**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.

C5 Requirements	Azure Activity	Test Result
Meta data must be deleted immediately once it is no longer required to fulfill the legitimate purpose according to this requirement. The period of time during which meta data is retained is determined by the cloud provider. It is reasonably related to the purposes pursued with the collection of meta data.		
RB-12 The cloud provider maintains a list of all assets critical in terms of logging and monitoring and reviews this list for their currency and correctness at regular intervals. For these critical assets, advanced logging and monitoring safeguards were defined.	**SOC2 - 2.** Azure services maintain an inventory of key information assets. Procedures to review the inventory on a monthly basis are established. **VM - 1.** Azure platform components are configured to log and collect security events.	No exceptions noted.
RB-13 The generated logs are stored on central logging servers on which they are protected against unauthorized access and changes. Logged data must be deleted immediately once they are no longer required to fulfill the purpose. Authentication takes place between the logging servers and the logged assets in order to protect the integrity and authenticity of the transmitted and stored information. The transmission is encrypted that conforms to the state of the art or via a separate administration network (out-of-band management).	**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. **CCM - 3.** 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.	No exceptions noted.

C5 Requirements	Azure Activity	Test Result
RB-14 The generated logs allow for a clear identification of user access to the tenant level in order to support (forensic) analyses in the case of a security incident.	**CCM - 9.** 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.
RB-15 The access and management of the logging and monitoring functionalities is limited to selected and authorized employees of the cloud provider. Changes to the logging and monitoring are checked by independent and authorized employees and approved beforehand.	**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. **CCM - 3.** 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. **D&T Note:** Changes made to the Azure logging and monitoring infrastructure were not in scope of the examination performed. However, it was tested that access is restricted to logging and monitoring infrastructure to an independent authorized team, as part of control C5 - 6, reducing the risk events impacting the infrastructure would go unnoticed as required. Thus, we can conclude that the design is appropriate to meet the C5 Objective 5.6.	No exceptions noted.
RB-16 The availability of the logging and monitoring software is monitored independently. In case the logging and monitoring software fails, the responsible employees are informed immediately.	**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.
RB-17 Policies and instructions with technical and organizational safeguards are documented, communicated and provided according to SA-01 in order to ensure the prompt identification and addressing of vulnerabilities over all levels of the cloud	**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.

C5 Requirements	Azure Activity	Test Result
service, for which they are responsible. The safeguards include among other things: • Regular identification and analysis of vulnerabilities, • Regular follow-up of safeguards in order to address identified safeguards (e.g., installation of security updates according to internal target specifications).		
RB-18 The cloud provider has penetration tests performed by qualified internal personnel or external service providers at least once a year. The penetration tests are carried out according to documented test methods and include the infrastructure components defined to be critical to the secure operation of the cloud service, which were identified as such as part of a risk analysis. Type, scope, time / period of time and results are documented comprehensibly for an independent third party. Determinations from the penetration tests are assessed and, in case of medium or high criticality regarding the confidentiality, integrity or availability of the cloud service, followed up and remedied. The assessment of the criticality and the mitigating safeguards for the individual determinations are documented.	**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.

C5 Requirements	Azure Activity	Test Result
RB-19 Policies and instructions with technical and organizational safeguards for the handling of critical vulnerabilities are documented, communicated and provided according to SA-01. The safeguards are coordinated with the activities of the change management and the incident 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.	No exceptions noted.
RB-20 The cloud customer is informed by the cloud provider of the status of the incidents affecting them in a regular and an appropriate form that corresponds to the contractual agreements or is involved into corresponding remedial actions. As soon as an incident was remedied from the cloud provider's point of view, the cloud customer is informed of the safeguards taken. This information is sufficiently detailed so that the cloud customer can use it in their security 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. **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.
RB-21 The IT systems which the cloud provider uses for the development and rendering of the cloud service are checked automatically for known vulnerabilities at least once a month. In the event of deviations from the expected configurations (for example, the expected patch level), the reasons for this are analyzed in a timely manner and the deviations remedied or documented	**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.	No exceptions noted.

C5 Requirements	Azure Activity	Test Result
according to the exception process (see SA-03).	**D&T Note:** Azure performs quarterly vulnerability scans on its production environment rather than the monthly scans. The production environment is continuously monitored for security and baseline configurations. Additionally, Azure development machines were not in scope of the examination as the development environment is isolated from the production environment. Our testing corroborates that changes developed on the development machines go through standard change management procedures including testing, scanning, and approval, prior to deployment in the production environment. Thus, we can conclude that the design is appropriate to meet the C5 Objective 5.6.	
RB-22 System components which are used for the rendering of the cloud service are hardened according to generally established and accepted industry standards. The hardening instructions used are documented as well as the implementation status.	**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.
RB-23 Data is separated securely and strictly on jointly used virtual and physical resources (storage network, memory) according to a documented concept in order to guarantee the confidentiality and integrity of the stored and processed data.	**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.

IDM: Identity and Access Management

Control Objective 5.7: Securing the authorization and authentication of users of the cloud provider (usually privileged user) and the cloud customer in order to prevent unauthorized access.

C5 Requirements	Azure Activity	Test Result
IDM-01 A role and rights concept based on the business and security requirements of the cloud provider as well as a policy for the management of system and data access authorizations are documented, communicated and provided according to SA-01 and address the following areas: • Granting and change (provisioning) of data access authorizations on the basis of the "least-privilege principle") and as is necessary for performing the required tasks ("need-to-know principle"), • Separation of functions between operative and controlling functions (also referred to as "separation of duties"), • Separation of functions in the administration of roles, approval and granting of data access authorizations, • Regular review of granted authorizations, • Withdrawal of authorizations (de-provisioning) in case of changes to the employment relationship, • Requirements for the approval and documentation of the management of system and data access authorizations.	**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.
IDM-02 System access authorizations for users under the responsibility of the cloud provider (internal and external employees) are granted in a formal procedure.	**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 Requirements	Azure Activity	Test Result
Organizational and / or technical safeguards make sure that unique user IDs which clearly identify each user are granted.	**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 - 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.	
IDM-03 Granting and change of data access authorizations for users under the responsibility of the cloud provider comply with the policy for the management of system and data access authorizations. Organizational and / or technical safeguards make sure that the granted access authorizations meet the following requirements: • Data access authorizations comply with the "least- Privilege principle"). • When granting data access authorizations, only access authorizations necessary to perform the corresponding tasks should be granted ("need-to- know principle"). • Formal approval is given by an authorized person, before the data access authorizations are set up (i. e. before the user can access data of the cloud customers	**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 to automatically disable Active Directory (AD) accounts and manually remove any non-AD accounts upon user's leave date are in place. **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. **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.	No exceptions noted.

C5 Requirements	Azure Activity	Test Result
or components of the shared IT infrastructure) • Technically assigned data access authorizations which do not exceed the formal approval.		
IDM-04 Data access authorizations of users under the cloud provider's responsibility (internal and external employees) are withdrawn in the case of changes to the employment relationship (dismissal, transfer, longer period of absence / sabbatical / parental leave) promptly, but 30 days after its coming into force at the latest and / or suspended temporarily. Any access is deactivated completely as soon as the employment relationship has expired.	**OA - 3.** Procedures to automatically disable Active Directory (AD) accounts and manually remove any non-AD accounts upon user's leave date are in place. **OA - 6.** Production domain-level user accounts for domains where passwords are in use are disabled after 90 days of inactivity. **OA - 11.** Procedures have been established to disable access to network devices in the scope boundary for terminated users on a timely basis.	No exceptions noted.
IDM-05 Data access authorizations of users under the cloud provider's responsibility (internal and external employees) are reviewed at least once a year in order to adjust them promptly to changes to the employment relationship (dismissal, transfer, longer period of absence / sabbatical / parental leave). The review is performed by persons authorized to do so from corresponding part of the cloud provider, who are able to review the appropriateness of the granted authorizations due to their knowledge of the 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. **OA - 12.** A quarterly review to validate the appropriateness of access to network devices in the scope boundary is performed by FTE managers.	No exceptions noted.

C5 Requirements	Azure Activity	Test Result
The review as well as the adjustments to the authorizations are documented comprehensibly.		
IDM-06 Granting and change of data access authorizations for internal and external users with administrative or extensive authorizations under the responsibility of the cloud provider comply with the policy or the management of system and data access authorizations (see IDM-01) or a separate policy. The authorizations are granted in a personalized manner and as is necessary for performing the corresponding tasks ("need-to-know principle"). Organizational and / or technical safeguards make sure that granting these authorizations does not result in undesired, critical combinations which violate the principle of the separation of duties (e.g., assigning authorizations for the administration of both the database and the operating system). If this is not possible in certain selected cases, appropriate, compensating controls are established in order to identify any misuse of these authorizations (e.g., logging and monitoring by an SIEM (security information and event management) solution).	**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. **CM - 3.** Responsibilities for requesting, approving, and implementing changes to the Azure platform are segregated among designated personnel. **VM - 2.** Administrator activity in the Azure platform is logged.	No exceptions noted.
IDM-07 Secret authentication credentials (e.g., passwords, certificates, security token) is assigned to internal and external users of the cloud provider or cloud customer, provided that this is subject to organizational	**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.	No exceptions noted.

C5 Requirements	Azure Activity	Test Result
or technical procedures of the cloud provider, in a proper organized procedure which ensures the confidentiality of the information. If it is assigned initially, it is valid only temporarily, but not longer than 14 days. Moreover, users are forced to change it when using it for the first time. Access of the cloud provider to the authentication information of the cloud customer is strictly regulated, communicated with the cloud customer and only takes place if it is necessary to perform the corresponding tasks ("need-to-know principle"). Access is documented and reported to the cloud customer.	**OA - 14.** Access to network devices in the scope boundary requires two-factor authentication and / or other secure mechanisms. **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 - 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. **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. Azure Active Directory 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. **D&T Note:** The initial password issued to internal users to access Azure production environment does not expire within 14 days, as specified by C5 Requirement IDM-07. However, initial temporary passwords follow the standard Microsoft password policy for age, length and complexity, and users are required to change temporary passwords at first login. 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.	

C5 Requirements	Azure Activity	Test Result
IDM-08 The confidentiality of the login information of internal and external users under the cloud provider's responsibility is protected by the following safeguards: • Identity check by trusted procedures, • Use of recognized industry standards for the authentication and authorization (e.g., multi- factor authentication, no use of jointly used authentication information, automatic expiry). • Multi-factor authentication for administrators of the cloud provider (e.g., using a smart card or biometric characteristics) is absolutely necessary.	**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 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. Azure Active Directory 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 Requirements	Azure Activity	Test Result
IDM-09 The use of emergency users (for activities which cannot be carried out with personalized, administrative users, see IDM-06) is documented, to be justified and requires the approval by an authorized person, which takes the principle of the separation of functions into account. The emergency user is only activated as long as it is necessary to perform the corresponding tasks.	**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.
IDM-10. Access to information and application functions is limited by technical safeguards with which the role and rights concept is implemented.	**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. **IS - 3.** Management has established defined roles and responsibilities to oversee implementation of the Security Policy across Azure.	No exceptions noted.
IDM-11. Security parameters on the network, operating system (host and guest), database and application level (where relevant to the cloud service) are configured appropriately to avoid unauthorized access. If no two-factor authentication or use of one-time passwords is possible, the use of secure passwords on all levels and devices (including mobile devices) under the cloud provider's responsibility is forced technically or must be ensured organizationally in a password policy. The targets must at least meet the following requirements: • Minimum password length of 8 characters,	**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. **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. Azure Active Directory password policy requirements are enforced on the new passwords supplied by customer administrators within SSPR portal. New	No exceptions noted.

C5 Requirements	Azure Activity	Test Result
• At least two of the following character types must be included: Capital letters, minor letters, special characters and numbers, • Maximum validity of 90 days, minimum validity of 1 day • Password history of 6 • Transmission and storage of the passwords in an encrypted procedure that conforms to the state of the art.	passwords supplied by customer administrators are protected during transmission over external networks.	
IDM-12. The use of service programs and management consoles (e.g., for the management of the hypervisor or virtual machines), which allow extensive access to the data of the cloud customers, is restricted to authorized persons. Granting and changes to corresponding data access authorizations comply with the policy for the management of system and data access authorizations. Access is controlled by means of strong authentication techniques, including multi-factor authentication (see KOS-06).	**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 - 8.** Authentication over an encrypted Remote Desktop Connection is used for administrator access to the production environment. **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. Azure Active Directory 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 Requirements	Azure Activity	Test Result
IDM-13. Access to the source code and supplementary information that is relevant to the development of the cloud service (e.g., architecture documentation, test plans) is granted restrictively and monitored in order to prevent unauthorized functions from being introduced and unintended changes from being made.	**SDL- 5.** A centralized repository is used for managing source code changes to the Azure platform. Procedures are established to authorize Azure personnel based on their role to submit source code changes.	No exceptions noted.

KRY: Cryptography and Key Management

Control Objective 5.8: Guaranteeing the appropriate and effective use of cryptography in order to protect the security of information.

C5 Requirements	Azure Activity	Test Result
KRY-01 Policies and instructions with technical and organizational safeguards for encryption procedures and key management are documented, communicated and provided according to SA-01, in which the following aspects are described: • Using strong encryption procedures (e.g., AES) and the use of secure network protocols that correspond to the state of the art (e.g., TLS, Ipsec, SSH), • Risk-based regulations for the use of encryption which are compared to schemes for the classification of information and take the communication channel, type, strength and quality of the encryption into account,	**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.

C5 Requirements	Azure Activity	Test Result
• Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys, • Taking the relevant legal and regulatory obligations and requirements into consideration.		
KRY-02 Procedures and technical safeguards for strong encryption and authentication for the transmission of data of the cloud customers (e.g., electronic messages transported via public networks) are established.	**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. **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.
KRY-03 Procedures and technical safeguards for the encryption of sensitive data of the cloud customers for the storage are established. Exceptions apply to data that cannot be encrypted for the rendering of the cloud service for functional reasons. The private keys used for encryption are known only to the customer according to applicable legal and regulatory obligations and requirements. Exceptions (e.g., use of a master key by the cloud provider) are based on a controlled procedure and must be agreed upon jointly 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 - 13.** Production data on backup media is encrypted. **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.	No exceptions noted.

C5 Requirements	Azure Activity	Test Result
KRY-04 Procedures and technical safeguards for secure key management 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 for customers and third parties involved, • Secure storage of own keys (not those of the cloud customers or other third parties) including the description as to how authorized users are granted access, • Changing or updating cryptographic keys including policies defining under which conditions and in which manner the changes and / or updates are to be realized, • Handling of compromised keys, • Withdrawal and deletion of keys, for example in the case of compromising or staff changes, • Storage of the keys of the cloud users not at the cloud provider (i. e. at the cloud user or a trusted third party).	**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 - 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. Keys must have identifiable owners (binding keys to identities) and key management policies.	No exceptions noted.

KOS: Communication Security

Control Objective 5.9: Ensuring the protection of information in networks and the corresponding information-processing systems.

C5 Requirements	Azure Activity	Test Result
KOS-01 Based on the results of a risk analysis carried out according to OIS-05, the cloud 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 (e.g., by MAC spoofing and ARP poisoning attacks) and / or Distributed Denial- of-Service (DDoS) attacks.	**OA - 16.** Network filtering to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted service components is implemented.	No exceptions noted.
KOS-02 Physical and virtualized network environments are designed and configured in such a way that the connections between trusted and untrusted networks must be restricted and monitored. At defined intervals, it is reviewed whether the use of all services, logs and ports serve a real commercial purpose. In addition, the review also includes the justifications for compensating controls for the use of logs which are considered to be insecure.	**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. **OA - 18.** Azure network is segregated to separate customer traffic from management traffic.	No exceptions noted.
KOS-03 Each network perimeter is controlled by security gateways. The system access authorization for cross- network access is based on a security assessment on the basis of the customer requirements.	**OA - 16.** Network filtering to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted service components is implemented. **OA - 18.** Azure network is segregated to separate customer traffic from management traffic.	No exceptions noted.

C5 Requirements	Azure Activity	Test Result
KOS-04 There are separate networks for the administrative management of the infrastructure and for the operation of management consoles, which are separated logically or physically by the network of the cloud customers and are protected against unauthorized access by means of multi-factor authentication (see IDM-17). Networks which are used for the purposes of the migration or the generation of virtual machines must also be separated physically or logically by other networks.	**OA - 18.** Azure network is segregated to separate customer traffic from management traffic.	No exceptions noted.
KOS - 05 The data traffic in jointly used network environments is segregated according to documented concept for the logical segmentation between the cloud customers on the network level in order to guarantee the confidentiality and integrity of the data transmitted.	**DS - 16.** Each Online Service's customer's data is segregated from other Online Services' customers' data, either logically or physically. **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. Keys must have identifiable owners (binding keys to identities) and key management policies. **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.
KOS - 06 The architecture of the network is documented comprehensibly and currently (e.g., in the form of diagrams) in order to avoid errors in the management during live	**C5 - 3.** The architecture of the Azure production network is documented as part of the inventory process. Metadata describing the network attributes (i.e.	No exceptions noted.

C5 Requirements	Azure Activity	Test Result
operation and ensure timely restoration according to the contractual duties in the event of damage. Different environments (e.g., administration network and shared network segments) and data flows become apparent from the documentation. Furthermore, the geographical locations, in which the data is stored, are specified.	location, tier, and connections) are dynamically generated and updated as part of standard operations.	
KOS - 07 Policies and instructions with technical and organizational safeguards in order to protect the transmission of data against unauthorized interception, manipulation, copying, modification, redirection or destruction (e.g., use of encryption) are documented, communicated and provided according to SA-01. The policy and instructions establish a reference to the classification of information (see AM-05).	**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.
KOS - 08 The non-disclosure or confidentiality agreements to be concluded with internal employees, external service providers and suppliers of the cloud provider are based on the requirements of the cloud provider in order to protect confidential data and business details. The requirements must be identified, documented and reviewed at regular intervals (at least once a year). If the review	**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 Requirements	Azure Activity	Test Result
shows that the requirements have to be adjusted, new non-disclosure or confidentiality agreements are concluded with the internal employees, the external service providers and the suppliers of the cloud provider. The non-disclosure or confidentiality agreements must be signed by internal employees, external service providers or suppliers of the cloud provider prior to the start of the contract relationship and / or before access to data of the cloud users is granted.	**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 - 7.** Azure maintains and communicates the confidentiality and related security obligations for customer data via the Microsoft Trust Center. **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.	

PI: Portability and Interoperability

Control Objective 5.10: Allowing the property to be able to securely operate the service on different IT platforms as well as the possibility of securely connecting different IT platforms and terminating the service.

C5 Requirements	Azure Activity	Test Result
PI-01 In order to guarantee the interoperability of cloud services, data regarding documented input and output interfaces and in recognized industry standards (e.g., the Open Virtualization Format for virtual appliances) is available in order to support the communication between different components and the migration of applications.	**CCM - 6.** Azure has published a standard set of APIs with an ecosystem of tools and libraries on the Azure Portal. **OA - 19.** Microsoft Azure has published virtualization industry standards supported within its environment.	No exceptions noted.

C5 Requirements	Azure Activity	Test Result
PI-02 At the end of the contract, the cloud customer can request the data to which they are entitled according to the contractual framework conditions, from the cloud provider and receives them in processable electronic standard formats such as CSV or XML.	**SOC2 - 28.** Customer data is accessible within agreed upon services in data formats compatible with providing those services.	No exceptions noted.
PI-03 If no individual agreements between the cloud provider and cloud customer regulate the interoperability and portability of the data, policies and instructions with technical and organizational safeguards are documented, communicated and provided according to SA-01 in order to ensure the respective requirements and duties of the cloud customer.	**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-04 The cloud provider uses secure network protocols for the import and export of information as well as for the management of the service in order to ensure the integrity, confidentiality and availability of the transported data.	**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. **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.	No exceptions noted.

C5 Requirements	Azure Activity	Test Result
PI-05 Both when changing the storage media for maintenance purposes and upon request of the cloud customer or the termination of the contract relationship, the content data of the cloud customer, including the data backups and the meta data (as soon as they are no longer required for the proper documentation of the accounting and billing), is deleted completely. The methods used for this (e.g., by overwriting data several times, deletion of the key) prevent the data from being restored via forensic methods.	**DS - 10.** Hard Disk Drive destruction guidelines for the disposal of Hard Drives have been established. **DS - 12.** Offsite backup tape destruction guidelines have been established and destruction certificates for expired backup tapes are retained. **DS - 15.** Customer data is retained and removed per the defined terms within the Microsoft Online Services Terms (OST), when a customer's subscription expires, or is terminated.	No exceptions noted.

BEI: Procurement, Development and Maintenance of Information Systems

Control Objective 5.11: Complying with the security targets in case of new developments and procurement of information systems as well as changes.

C5 Requirements	Azure Activity	Test Result
BEI-01 Policies and instructions with technical and organizational safeguards for the proper development and / or procurement of information systems for the development or operation of the cloud service, including middleware, databases, operating systems and network components are documented, communicated and provided according to SA-01.	**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 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.	No exceptions noted.

C5 Requirements	Azure Activity	Test Result
The policies and instructions describe at least the following aspects: • Security in software development methods in compliance with security standards established in the industry (e.g., OWASP for web applications), • Security of the development environment (e.g., separate development / test / production environments), • Programming policies for each programming language used (e.g., regarding buffer overflows, hiding internal object references towards users), • Security in version control.	Keys must have identifiable owners (binding keys to identities) and key management policies. **SDL - 1.** Development of new features and major changes to the Azure platform follow a defined approach based on the Microsoft Secure Development Lifecycle (SDL) methodology. **SDL - 2.** Applicable operational security and internal control requirements are documented and approved for major releases prior to production deployment. **SDL - 7.** The SDL review for each service with a major release is performed and completed on a semi-annual basis, and signed off on by designated owners. **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.	
BEI-02 If the development of the cloud service (or parts thereof) is outsourced regarding the design, development, test and / or provision of source code of the cloud service, a high level of security is required. Therefore, at least the following aspects must be agreed upon contractually between the cloud provider and external service providers: • Requirements for a secure software development process (especially design, development and testing) • Provision of evidence demonstrating that adequate testing was carried out by the external service provider	Not Applicable as Microsoft Azure does not outsource development work.	No exceptions noted.

C5 Requirements	Azure Activity	Test Result
• Acceptance test of the quality of the services rendered according to the functional and non- functional requirements agreed upon • The right to subject the development process and controls to testing, also on a random basis		
BEI-03 Policies and instructions with technical and organizational safeguards for the proper management of changes to information systems for the development or operation of the cloud service, including middleware, databases, operating systems and network components are documented, communicated and provided according to SA-01. At least the following aspects are to be taken into account in this respect: • Criteria for the classification and prioritization of changes and related requirements for the type and scope of tests to be carried out and permits to be obtained, • Requirements for the notification of affected cloud customers according to the contractual agreements, • Requirements for the documentation of tests as well as for the application and permit of changes, • Requirements for the documentation of changes to the system, operating and user documentation.	**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 to the Azure platform have been documented and communicated. **CM - 9.** Datacenter change requests are classified, documented, and approved by the Operations Management Team. **CM - 11.** Change management processes include established workflows and procedures to address emergency change requests. **CM - 6.** Procedures to manage changes to network devices in the scope boundary have been established.	No exceptions noted.

C5 Requirements	Azure Activity	Test Result
BEI-04 The principal of a change performs a risk assessment beforehand. All configuration objects which might be affected by the change are assessed with regard to potential impacts. The result of the risk assessment is documented appropriately and comprehensively.	**CM - 2.** Key stakeholders approve changes prior to release into production based on documented change management procedures.	No exceptions noted.
BEI-05 All changes are categorized on the basis of a risk assessment (e.g., as insignificant, significant or far- reaching impacts) in order to obtain an appropriate authorization prior to making the change available to the production environment.	**CM - 1.** Procedures for managing different types of changes to the Azure platform have been documented and communicated. **CM - 2.** Key stakeholders approve changes prior to 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.
BEI-06 All changes are prioritized on the basis of a risk assessment (e.g., as low, normal, high, emergency) in order to obtain an appropriate authorization prior to making the change available to the production environment.	**CM - 1.** Procedures for managing different types of changes to the Azure platform have been documented and communicated. **CM - 2.** Key stakeholders approve changes prior to 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 - 9.** Datacenter change requests are classified, documented, and approved by the Operations Management Team.	No exceptions noted.

C5 Requirements	Azure Activity	Test Result
BEI-07 All changes to the cloud service are subjected to tests (e.g., for integration, regression, security and user acceptance) during the development and before they are made available to the production environment. The tests are carried out by adequately qualified personnel of the cloud provider. According to the service level agreement (SLA), changes are also tested by the customers (tenants) suitable for this.	**CM - 1.** Procedures for managing different types of changes to the Azure platform have been documented and communicated. **CM - 2.** Key stakeholders approve changes prior to 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 - 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.	No exceptions noted.
BEI-08 Processes are defined in order to be able to roll back required changes as a result of errors or security concerns and restore affected systems or services into its previous state.	**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.
BEI-09 Before a change is released to the production environment, it must be reviewed by an authorized body or a corresponding committee whether the planned tests have been completed successfully and the required approvals are granted.	**CM - 1.** Procedures for managing different types of changes to the Azure platform have been documented and communicated. **CM - 2.** Key stakeholders approve changes prior to release into production based on documented change management procedures.	No exceptions noted.

C5 Requirements	Azure Activity	Test Result
	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. **CM - 9.** Datacenter change requests are classified, documented, and approved by the Operations Management Team.	
BEI-10 Emergency changes are to be classified as such by the change manager who creates the change documentation before applying the change to the production environment. Afterwards (e.g., within 5 working days), the change manager supplements the change documentation with a justification and the result of the application of the emergency change. This justification must show why the regular change process could not have been run through and what the consequences of a delay resulting from compliance with the regular process would have been. The change documentation is forwarded to the customers concerned and a subsequent release by authorized bodies is obtained according to the contractual agreements.	**CM - 11.** Change management processes include established workflows and procedures to address emergency change requests. **D&T Note:** The addition of a justification to emergency changes to the change documentation was not in scope of the examination performed. However, emergency changes are only made by internal services that do not contain or impact any customer data. Thus, we can conclude that the design is appropriate to meet the C5 objective 5.11.	No exceptions noted.

C5 Requirements	Azure Activity	Test Result
BEI-11 Production environments are separated physically or logically by non-production environments in order to avoid unauthorized access or changes to the production data. Production data is not replicated in test or development environments in order to maintain 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.	No exceptions noted.
BEI-12 Change management procedures include role-based authorizations in order to ensure an appropriate separation of duties regarding the development, release and migration of changes between the environments.	**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. **CM - 3.** Responsibilities for requesting, approving, and implementing changes to the Azure platform are segregated among designated personnel. **SDL - 3.** Responsibilities for submitting and approving production deployments are segregated within the Azure teams.	No exceptions noted.

DLL: Control and Monitoring of Service Providers and Suppliers

Control Objective 5.12: Ensuring the protection of information which can be accessed by the service providers and / or suppliers of the cloud provider (subcontractors) and monitoring the services and security requirements agreed upon.

C5 Requirements	Azure Activity	Test Result
DLL-01 Policies and instructions for ensuring the protection of information accessed by other third parties (e.g., service providers and / or suppliers of the cloud provider), who contribute significant parts to the development or operation of the cloud	**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.

C5 Requirements	Azure Activity	Test Result
service, are documented, communicated and provided according to SA-01. The corresponding controls are used to mitigate risks which may result from the potential access to information of the cloud customers. The following aspects are at least to be taken into account for this: • Definition and description of minimum security requirements with regard to the information processed, which are based on recognized industry standards such as ISO / IEC 27001, • Legal and regulatory requirements, including data protection, intellectual property right, copyright, handling of meta data (see RB-11) as well as a description as to how they are ensured (e.g., site of data processing and liability, see surrounding parameters for transparency), • Requirements for incident and vulnerability management (especially notifications and collaborations when eliminating malfunctions), • Disclosure and contractual obligation to the minimum security requirements also to subcontractors if they do not only contribute insignificant parts to the development or operation of the cloud service (e.g., service provider of the computing center). The definition of the requirements is integrated into the risk management of the cloud provider.		

C5 Requirements	Azure Activity	Test Result
According to requirement OIS-07, they are checked at regular intervals for their appropriateness.		
DLL-02 Procedures for the regular monitoring and review of agreed services and security requirements of third parties (e.g., service providers and / or suppliers of the cloud provider) who contribute essential parts to the development or operation of the cloud service are established. The safeguards include at least the following aspects: • Regular review of service reports (e.g., SLA reports) if they are provided by third parties, • Review of security-relevant incidents, operational disruptions or failures and interruptions that are related to the service, • Unscheduled reviews after essential changes to the requirements or environment. The essentiality must be assessed by the cloud provider and documented comprehensibly for audits. Identified deviations are subjected to a risk analysis according to requirement OIS-07 in order to effectively address them by mitigating safeguards in a timely manner.	**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. **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.	No exceptions noted.

SIM: Security Incident Management

Control Objective 5.13: Ensuring a consistent approach regarding the monitoring, recording, assessment, communication and escalation of security incidents.

C5 Requirements	Azure Activity	Test Result
SIM-01 Policies and instructions with technical and organizational safeguards are documented, communicated and provided according to SA-01 in order to ensure a fast, effective and proper response to all known security incidents. On the part of the cloud provider, at least the roles listed in OIS-01 must be filled, requirements for the classification, prioritization and escalation of security incidents defined and interfaces with the incident management and the business continuity management created. In addition to this, the cloud provider has established a "computer emergency response team" (CERT), which contributes to the coordinated solution of specific security incidents. Customers affected by security incidents are informed in a timely manner and appropriate form.	**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. **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.
SIM-02 All customer systems are classified according to the agreements (SLA) between the cloud provider and cloud customer regarding the criticality for the rendering of services. The assignment of classifications is reviewed regularly as well as after essential changes / events for all customer systems. Deviations are followed up and eliminated in a timely manner. Moreover, the classification shows which parameters regarding the	**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. **D&T Note:** The review of classification of customer systems infrastructure and remediation of any deviations identified as part of the review, were not in scope of the examination performed. However, we tested that customers are provided with agreements stating their system classification and are notified on any changes	No exceptions noted.

C5 Requirements	Azure Activity	Test Result
recovery of a system were agreed upon with the cloud customer.	made to the system. Thus, we can conclude that the design is appropriate to meet the C5 objective 5.13.	
SIM-03 Events which could represent a security incident are classified, prioritized and subjected to a cause analysis by qualified personnel of the cloud provider or in connection with external security service providers.	**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.
SIM-04 After a security incident has been processed, the solution is documented according to the contractual agreements and the report is forwarded for final information or, if necessary, as confirmation to the customers affected.	**CCM - 9.** Microsoft Azure has established forensic procedures to support potential legal action after an information security incident. **IM - 4.** Incident post-mortem activities for severe incidents impacting the Azure environment are conducted. **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.
SIM-05 Logged incidents are centrally aggregated and consolidated (event correlation). Rules for identifying relations between incidents and assessing them according to their criticality are implemented. These incidents are handled according to the security incident management process.	**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.

C5 Requirements	Azure Activity	Test Result
SIM-06 The employees and external business partners are informed of their duties. If necessary, they agree to or commit themselves contractually to promptly report all security events to a previously specified central body. Furthermore, information is provided that "incorrect notifications" of events which have not turned out to be incidents afterwards, do not have any negative consequences for the employees.	**IS - 3.** Management has established defined roles and responsibilities to oversee implementation of the Security Policy across Azure. **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.
SIM-07 Mechanisms are in place to be able to measure and monitor the type and scope of the security incidents as well as to report them to supporting bodies. The information gained from the evaluation is used to identify recurring incidents or incidents involving significant consequences and to determine the need for advanced safeguards.	**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: Strategic establishment and control of a Business Continuity Management (BCM) plan. Planning, implementing and testing business continuity concept as well as incorporating safeguards in order to ensure and maintain operations.

C5 Requirements	Azure Activity	Test Result
BCM-01 The top management (and / or a member of the top management) is specified as the process owner of the business continuity and contingency management and bears the responsibility for the establishment of the process in the company and compliance with the policies. They must ensure that adequate resources are made available for an effective process. Members of the top management and persons in other relevant leadership positions demonstrate leadership and commitment with respect to this topic, for example by asking and / or encouraging the employees to actively contribute to the effectiveness of the business continuity and contingency 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.** Datacenter Business Continuity Management (BCM) program to respond to Microsoft's Enterprise Business Continuance Initiative has been implemented and includes documented procedures for performing a Business Impact Analysis, establishing Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), 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 a major disruptive events.	No exceptions noted.
BCM-02 Policies and instructions for determining impacts of possible malfunctions of the cloud service or company are documented, communicated and provided according to SA-01. At least the following aspects are taken into consideration: • Possible scenarios based on a risk analysis (e.g., loss of personnel, failure of building, infrastructure and service providers),	**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.** Datacenter Business Continuity Management (BCM) program to respond to Microsoft's Enterprise Business Continuance Initiative has been implemented and includes documented procedures for performing a Business Impact Analysis, establishing Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), mapping processes to pre-defined enterprise functions, establishing recovery strategies as well as developing and conducting test scenarios that	No exceptions noted.

C5 Requirements	Azure Activity	Test Result
• Identification of critical products and services, • Identification of dependencies, including the processes (incl. the resources required for this), applications, business partners and third parties, • Identification of threats to critical products and services, • Determination of consequences resulting from planned and unplanned malfunctions and changes over time, • Determination of the maximum acceptable duration of malfunctions, • Determination of the priorities for the restoration, • Determination of time-limited targets for the recovery of critical products and services within the maximum acceptable period of time (recovery time objective, RTO); • Determination of time-limited targets for the maximum acceptable period of time during which data is lost and cannot be restored (recovery point objective, RPO); • Estimation of the resources required for recovery.	enable the BCM program to mitigate risks and vulnerabilities and respond to a major disruptive events.	
BCM-03 Based on the business impact analysis, a uniform framework for planning the business continuity and business plan is introduced, documented and applied in order to ensure that all plans (e.g., of the different sites of the cloud provider) are consistent.	**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.	No exceptions noted.

C5 Requirements	Azure Activity	Test Result
The planning depends on established standards which is documented comprehensibly in a "statement of applicability". Business continuity plans and contingency plans take the following aspects into consideration: • Defined purpose and scope by taking the relevant dependencies into account, • Accessibility and comprehensibility of the plans for persons who have to take action in line with these plans, • Ownership by at least one appointed person who is responsible for review, updating and approval, • Defined communication channels, roles and responsibilities including the notification of the customer, • Restoration procedures, manual temporary solutions and reference information (by taking the prioritization into account for the recovery of cloud infrastructure components and services as well as orienting to customers), • Methods used for the implementation of the plans, • Continuous improvement process of the plans, • Interfaces with the security incident 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 - 8.** 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.	

C5 Requirements	Azure Activity	Test Result
BCM-04. The business impact analysis as well as the business continuity plans and contingency plans are verified, updated and tested at regular intervals (at least once a year) or after essential organizational or environment-related changes. The tests also involve affected customers (tenants) and relevant third parties (e.g., critical suppliers). The tests are documented and results are taken into account for future business continuity safeguards.	**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 for different loss scenario. Each loss scenario is tested at least annually. Issues identified during testing are resolved and plans are updated accordingly.	No exceptions noted.
BCM-05. The supply of the computing centers (e.g., water, electricity, temperature and moisture control, telecommunications and Internet connection) is secured, monitored and is maintained and tested at regular intervals in order to guarantee continuous effectiveness. It has been designed with automatic fail-safe mechanisms and other redundancies. Maintenance is performed in compliance with the maintenance intervals and targets recommended by the suppliers as well as only by personnel authorized to do so. Maintenance protocols including any suspected or detected deficiencies are stored for the duration of the period of time previously agreed upon. After this period of time has expired, the maintenance protocols are destroyed properly and permanently.	**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.

SPN: Security Check and Verification

Control Objective 5.15: Checking and verifying that the information security safeguards are implemented and carried out in accordance with the organization-wide policies and instructions.

C5 Requirements	Azure Activity	Test Result
SPN-01 The top management is informed of the status of the information security on the basis of security checks by means of regular reports and is responsible for the prompt elimination of determinations resulting from them.	**IS - 3.** Management has established defined roles and responsibilities to oversee implementation of the Security Policy across Azure. **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.
SPN-02 Qualified personnel (e.g., internal revision) of the cloud provider or expert third parties commissioned by the cloud provider audit the compliance of the internal IT processes with the corresponding internal policies and standards as well as the legal, regulatory and statutory prescribed requirements relevant to the cloud service on an annual basis. The deviations identified are prioritized and, depending on their criticality, safeguards for their elimination are defined, followed up and implemented in a timely manner.	**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 - 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.

C5 Requirements	Azure Activity	Test Result
SPN-03 At least on an annual basis, qualified personnel (e.g., internal revision) of the cloud provider or expert third parties commissioned by the cloud provider audit the compliance of the IT systems, provided that they are completely or partially in the cloud provider's area of responsibility and are relevant to the development or operation of the cloud service, with the corresponding internal policies and standards as well as the legal, regulatory and statutory prescribed requirements relevant to the cloud service. The deviations identified are prioritized and, depending on their criticality, safeguards for their elimination are defined, followed up and implemented in a timely manner.	**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 - 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.

COM: Compliance and Data Protection

Control Objective 5.16: Avoiding violations against statutory or contractual duties with respect to information security.

C5 Requirements	Azure Activity	Test Result
COM-01 Legally, regulatory and statutory prescribed requirements, as well as the procedure to comply with these requirements and regulations must be identified, documented and updated regularly by the cloud provider for the cloud service related to the respective application.	**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.

C5 Requirements	Azure Activity	Test Result
COM-02 Independent audits and assessments of systems or components which contribute to the rendering of the cloud services are planned by the cloud provider in such a way that the following requirements are met: • There is only read access to software and data. • Activities which might impair the availability of the systems or components and thus result in a violation of the SLA are carried out outside regular business hours and / or not at load peak times. • The activities performed are logged and monitored.	**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 - 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.
COM-03 Audits and assessments of processes, IT systems and IT components, provided that they are completely or partially in the cloud provider's area of responsibility and are relevant to the development or operation of the cloud service, are carried out by independent third parties (e.g., certified public auditor) at least once a year in order to identify non-conformities with legally, regulatory and statutory prescribed requirements. The deviations identified are prioritized and, depending on their criticality, safeguards for their elimination are defined, followed up and implemented 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 - 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.

MDM: Mobile Device Management

Control Objective 5.17: Guaranteeing security when using mobile terminal devices in the cloud provider's area of responsibility for the access to IT systems in order to develop and operate the cloud service.

C5 Requirements	Azure Activity	Test Result
MDM-01 Policies and instructions with technical and organizational safeguards for the proper use of mobile terminal devices in the cloud provider's area of responsibility, which allow access to IT systems for the development and operation of the cloud service, are documented, communicated and provided according to SA-01. These policies and instructions include at least the following aspects, insofar as they are applicable to the cloud provider's situation: • Encryption of the devices and data transmission, • Increased access protection, • Extended identity and authorization management, • Ban on jailbreaking / rooting, • Installation only of approved applications from "App Stores" classified as trusted, • Bring your own device (BYOD) minimum requirements for private terminal devices.	**CCM - 1.** 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.

Part D: 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 the 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 the 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 the 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	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		of the security policy requirements were defined and documented.	
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 the management to gain an understanding of the processes for awareness and training on information security for employees, contractors, and third-party users. • Inspected training material to ascertain that it incorporated security policy requirements, 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 the management to understand the procedures in place for accessing the Azure production environment, including data backups and datacenters. • For a select 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 a list of current users with alias for Azure 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	• Inquired of the management if access requests require approval by the security group owner or asset owner using the account management tool.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	prior to provisioning employee, contractor, and service provider access to specific applications or information resources.	• For a sample security group, performed a walkthrough with the security group owner to ascertain that access to the security group was granted as per the approval rules configured. • For a select sample of security groups / individual user access, obtained and inspected approvals prior to provisioning access to specific applications or information resources.	
OA - 3	Procedures to automatically disable Active Directory (AD) accounts and manually remove any non-AD accounts upon user's leave date are in place.	• Inquired of the Operations team if procedures for disabling terminated user accounts within a defined time period after the user's termination date are established. • Compared the list of users from the relevant production domains against the HR termination report. Matches from the domain users to the terminated users were checked in the Microsoft Global Address List, HR application, account creation date, and / or access request tickets to ascertain if access was still appropriate. • Selected a sample of terminated users and obtained and inspected Active Directory (AD) domain logs showing that corporate accounts and AD production domain accounts were disabled within 5 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	• Inquired of the 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.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	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.	• 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 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.	
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. • For a select sample of managers reviewing Azure access, obtained and inspected the review log to ascertain whether reviews were performed for the managers' direct reports, and completed with implementation of identified changes.	No exceptions noted.
OA - 6	Production domain-level user accounts for domains where passwords are in use are disabled after 90 days of inactivity.	• Inquired of the Cloud + AI Security team if procedures are established for disabling user accounts inactive for 90 days in the production environment where passwords are in use. • Obtained and inspected applicable domain user listings, with last login and account status details, to ascertain that there were no active accounts with inactivity over 90 days.	No exceptions noted.
OA - 7	Procedures for granting Azure personnel temporary access to customer data and applications, upon appropriate approval for	• Inquired of the management to understand the procedures in place for granting and revoking temporary access to internal administration services.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	customer support or incident handling purposes, have been established.	• Performed a walkthrough with the control owner to ascertain that processes were in place to provision temporary access to customer data and applications upon approvals from designated personnel. • For a select 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.	
OA - 8	Authentication over an encrypted Remote Desktop Connection is used for administrator access to the production environment.	• Inquired of the process owners to understand the authentication enforced during an RDP session to production environment and encryption of an RDP session. • 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.	No exceptions noted.
OA - 9	User groups and Access Control Lists have been established to restrict access to network devices in the scope boundary.	• Inquired of the Networking team if user groups and Access Control Lists (ACLs) are established to restrict access to network devices. • Inquired if user groups were created and enforced via the Active Directory. • Obtained and inspected configuration for a sample of network devices, and ascertained that TACACS+ / RADIUS 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	• Inquired of the Networking team regarding the procedures in place to grant access to new users for network devices in the scope boundary.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	boundary upon receiving appropriate approvals.	• Observed the approval process to ascertain that access to a security group was granted upon approval from the network security group owner. • For a select sample of network security groups, sampled a user and ascertained that access was appropriate.	
OA - 11	Procedures have been established to disable access to network devices in the scope boundary for terminated users on a timely basis.	• Inquired of the Operations team if procedures are established for disabling terminated user accounts within a defined time period after the user's termination date. • Compared the list of users from the relevant production domains against the HR termination report. Matches from the domain users to the terminated users were checked in the Microsoft Global Address List, HR application, account creation date, and / or access request tickets to ascertain if access was still appropriate. • Selected a sample of terminated users and obtained and inspected Active Directory (AD) domain logs showing that corporate accounts and AD production domain accounts were disabled within 5 days of the user's termination date.	No exceptions noted.
OA - 12	A quarterly review to validate the appropriateness of access to network devices in the scope boundary is performed by FTE managers.	• Inquired of the Networking team if users' access to network devices is reviewed in accordance with documented procedures. • Inspected the Network Account Management SOP and ascertained that processes were established to review user access to network devices on a quarterly basis. • Inspected a sample of quarterly user access reviews and ascertained that the reviews were performed in accordance with documented procedures.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		• Selected a sample of users from the population of users reviewed in the above quarterly access reviews and ascertained that change requests, resulting from the reviews, were performed.	
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 the Networking team 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. • For a sampled hop-box server, performed a walkthrough to ascertain that remote access to network devices involved logging into a hop-box 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 select sample of hop-box 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.	No exceptions noted.
OA - 14	Access to network devices in the scope boundary requires two-	• Inquired of the Networking team if two-factor authentication is enforced for connecting to a network device.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	factor authentication and / or other secure mechanisms.	• For a sample 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+ or RADIUS servers.	
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 the Networking Team to gain an understanding of: – The network equipment where static passwords exist and the type of static accounts (e.g., root accounts, service accounts, system accounts) – Password rotation cadence of the accounts used to access the network devices – The process used to change the static passwords – The restriction of passwords to authorized individuals based on job responsibilities • 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.	**Exception Noted:** Exceptions were identified in the period previous to the current examination period. Evidence related to password rotation was not retained and not available for inspection to corroborate that the passwords were changed on a periodic basis. Per inquiry of management, remediation for this control was in progress from April 1, 2019 through June 30, 2019. D&T sampled 26 samples subsequent to June 30, 2019, and no additional exceptions were 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 the management regarding the packet filtering mechanisms implemented to restrict incoming and outgoing traffic. • Obtained and inspected the configuration files for a select set of nodes 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 the 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 the 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 the Azure Operations team to understand the various published virtualization industry standards supported within the Azure environment, and solution-specific virtualization hooks available for customer review. • Re-performed the control to ascertain that Azure published virtualization formats (e.g., Open Virtualization Format (OVF)) supported interoperability with third-party products such as	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		Oracle Virtual Box, VMware Workstation, and XenSource.	
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 the Azure Operations team 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. • Performed a walkthrough with the control owner to observe 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 select 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.	No exceptions noted.
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 the Azure Operations team 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. • Re-performed 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	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		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.	• Inquired of the Azure Operations team to understand the use of secure mechanisms such as encryption for communication between internal Azure components that involves customer data. • For a select sample of Azure platform components, inspected configurations and observed the use of secure encryption mechanisms for internal communication.	No exceptions noted.
DS - 4	Cryptographic controls are used for information protection within the Azure platform based on the Azure Cryptographic Policy and Key Management procedures. Keys must have identifiable owners (binding keys to identities) and key management policies.	• Inquired of the management regarding the policies and procedures in place for using cryptographic controls within the Azure environment. • For a select sample of major releases, ascertained that cryptographic policy requirements were enforced and required approvals were obtained for exceptions. • For a select sample of secrets from different Azure services using Secret Store, obtained and inspected secret store inventory details to ascertain that secrets were stored under service specific namespaces. • For a select sample of secrets from different Azure services using Key Vault, obtained and inspected secret configuration to ascertain that secrets were stored under service specific Vaults.	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	• Inquired of the 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	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	and backup errors are investigated and followed-up on appropriately.	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.	
DS - 6	Critical Azure components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services.	• Inquired about the redundancy mechanisms in place for key components within the production environment. • For a select 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 processing and storage, including data backups.	• Inquired about the redundancy mechanisms in place to replicate data stored across Azure services. • For a select sample of Storage accounts and SQL Databases, inspected configurations and ascertained that data was replicated across multiple nodes. • Obtained and inspected configurations for the selected sampled services to determine geographical region of the data processing and storage.	No exceptions noted.
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 the DPS team regarding the process for scheduling of backups of production database based on customer requests. • Inquired 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.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		• For a select 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 select sample of backup failures, obtained tickets / backup status showing resolution details.	
DS - 9	Backup restoration procedures are defined and backup data integrity checks are performed through standard restoration activities.	• Inquired of the DPS team 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 select 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.	No exceptions noted.
DS - 10	Hard Disk Drive destruction guidelines for the disposal of Hard Drives have been established.	• Inquired of the management to understand the process for hard disk drive disposal. • Obtained the population of hard disk drive disposals performed during the examination period, and judgmentally selected a sample of disposals. • For a select sample of disposals, obtained and inspected tickets to ascertain that the disposal followed the standard disposal process.	No exceptions noted.
DS - 11	Offsite backups are tracked and managed to maintain accuracy of the inventory information.	• Inquired of the DPS team if processes for tracking and managing offsite backups to maintain accuracy of the inventory information are established.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		• Obtained and inspected DPS operating procedures and ascertained that the process for transport of backup tapes offsite and verification of offsite inventory was documented. • For a select sample of daily backup transport / tape swap tickets, obtained and inspected discrepancy reports, to ascertain that discrepancies were escalated and resolved, where applicable.	
DS - 12	Offsite backup tape destruction guidelines have been established and destruction certificates for expired backup tapes are retained.	• Inquired of the DPS team if offsite backup tape destruction guidelines are established and destruction certificates for expired backup tapes are retained. • Obtained and inspected DPS SOPs and guidelines and ascertained that the process for destruction of backup tapes was documented. • For a select sample of media destruction requests, obtained and inspected media destruction evidence (i.e., request containing the list of expired tapes and corresponding destruction certificates) to ascertain that the destruction evidence was retained.	No exceptions noted.
DS - 13	Production data on backup media is encrypted.	• Inquired of the DPS team if production data is encrypted prior to storage on backup media. • For a select sample of servers, obtained and inspected data encryption configurations to ascertain that production data was encrypted. • Obtained and inspected the configuration settings for a select sample of backup encryption system instances to ascertain whether they are enabled to encrypt production data for tape backups.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
DS - 14	Azure services are configured to automatically restore customer services upon detection of hardware and system failures.	• Inquired about the failover mechanisms in place to automatically restore role instances upon detection of a hardware and system failure. • For a select sample of node instances, observed the health status and service healing history to ascertain that automatic restoration was occurring.	No exceptions noted.
DS - 15	Customer data is retained and removed per the defined terms within the Microsoft Online Services Terms (OST), when a customer's subscription expires, or is terminated.	• Inquired 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 subscription, ascertained that access to customer data was handled in accordance with Microsoft Online Services 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.	• Performed inquiry of the service owner to understand how the MSODS environment enforces logical or physical segregation of customer data. • Re-performed the control using test domains to ascertain that customer (tenant) data was segregated.	No exceptions noted.
CM - 1	Procedures for managing different types of changes to the Azure platform have been documented and communicated.	• Inquired of the 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	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		changes, including major release, minor release, hotfix, and configuration changes, were defined.	
CM - 2	Key stakeholders approve changes prior to release into production based on documented change management procedures.	• Inquired of the 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 - 3	Responsibilities for requesting, approving, and implementing changes to the Azure platform are segregated among designated personnel.	• Inquired of the 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.	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 the management about the procedures for managing various types of changes to the Microsoft Azure environment, including testing requirements.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		• 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.	
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 the 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 implemented changes were rolled back to their previous state in case of errors or security concerns. • Selected a sample of changes to production and ascertained that changes were reviewed prior to closure.	No exceptions noted.
CM - 6	Procedures to manage changes to network devices in the scope boundary have been established.	• Inquired of the Networking team regarding the procedures established for managing changes to network devices in the scope boundary. • Inspected network change management procedures, and for a select 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.

Control ID	Control Activity	Test Procedures	Results of Tests
CM - 7	Secure network configurations are applied and reviewed through defined change management procedures.	• Inquired of the Networking team if the implementation and review of secure network configuration standards are followed through defined change management procedures. • Inspected Azure Networking change 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 (e.g., IPAK team).	• Inquired of the Cloud + AI Security team 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. • Selected a sample of servers and inspected their configuration to ascertain that documented security configuration standards and technical baseline were implemented.	No exceptions noted.
CM - 9	Datacenter change requests are classified, documented, and approved by the Operations Management Team.	• Inquired of the Networking team if change requests are classified, documented, and approved by the Operations Management Team.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		• 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.	
CM - 10	Secure configurations for datacenter software are applied through defined change management procedures including documentation, testing and approval.	• Inquired of the Server Standards Team if server-based images (IPAKs) 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 - 11	Change management processes include established workflows and procedures to address emergency change requests.	• Inquired of the Networking team if procedures and workflows are established to address emergency change requests. • Inspected the Emergency Change Management Procedures and tested that procedures and workflows were established to address emergency change requests.	No exceptions noted.
SDL - 1	Development of new features and major changes to the Azure platform follow a defined approach based on the Microsoft	• Inquired of the management if the Microsoft SDL methodology for the development of new features and major changes to Microsoft Azure platform is followed.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	Secure Development Lifecycle (SDL) methodology.	• Obtained and inspected documentation to ascertain that an SDL methodology was defined to incorporate security practices as part of the development process. • For a select sample of changes made to production, obtained and inspected tickets to ascertain that documented procedures for testing were followed prior to deployment.	
SDL - 2	Applicable operational security and internal control requirements are documented and approved for major releases prior to production deployment.	• Inquired of the management regarding the process to identify and document applicable operational security and internal control requirements as part of the SDL process. • For a select sample of major releases, ascertained that operational security and internal control requirements were identified, documented, and approved by designated owners.	No exceptions noted.
SDL - 3	Responsibilities for submitting and approving production deployments are segregated within the Azure teams.	• Inquired of the service teams if responsibilities for production deployment are segregated within the Microsoft Azure teams. • For a select 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	• Inquired of the service teams if changes are developed and tested in separate environments prior to production deployment and production data is not replicated in test or development environments.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	in test or development environments.	• For a select 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 select sample of changes made to production, obtained and inspected tickets to ascertain that documented procedures for testing were followed prior to deployment.	
SDL - 5	A centralized repository for managing source code changes to the Azure platform is used. Procedures to authorize Azure personnel to submit source code changes based on their role, are established.	• Inquired of the service teams about the access control procedures for source code repository. • For a select sample of services, obtained and inspected security groups and membership to ascertain that access to the source code repository was restricted to authorized Azure personnel.	No exceptions noted.
SDL - 6	Source code builds are scanned for malware prior to release to production.	• Inquired of the service teams regarding the procedures in place to scan source code builds for malware. • For a select 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.
SDL - 7	The SDL review for each service with a major release is performed and completed on a	• Inquired of the management if an SDL review is performed at least semi-annually for each service with a major release and signed off by designated owners.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	semi-annual basis, and signed off on by designated owners.	• For a sample of services, obtained and inspected relevant SDL tickets with review and sign-off details to ascertain that an SDL review was completed in the past six months as per the SDL methodology, and sign-offs were obtained from designated owners.	
VM - 1	Azure platform components are configured to log and collect security events.	• Inquired of the management regarding security event logging configured for Azure services to enable detection of potential unauthorized or malicious activities. • For a select sample of services, obtained and inspected configurations and logs to ascertain that logging of key security events was enabled per documented procedures. • Inspected configurations and a sample notification to corroborate that security events generated alerts based on defined rulesets. • Observed the monitoring configuration to ascertain that a mechanism was in place to detect and resolve the activation or stopping of the logging process.	No exceptions noted.
VM - 2	Administrator activity in the Azure platform is logged.	• Inquired of the management regarding the mechanisms that are in place for logging administrator activities within Azure Service platform. • For a select sample of services, obtained and inspected security logs to ascertain that administrator events were logged to the centralized monitoring infrastructure.	No exceptions noted.
VM - 3	A monitoring system to monitor the Azure platform for potential malicious activity and intrusion	• Inquired of the management regarding the monitoring capabilities within the Azure environment	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	past service trust boundaries has been implemented.	to detect potential malicious activities and intrusions. • For a select sample of services, 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 to corroborate that they were up to date.	
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 the Microsoft Azure Incident Management Leads 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 the management regarding the patch management process within the Azure environment. • Inspected patch management SOP and ascertained that procedures for evaluating and implementing released patches within the Azure environment were established. • For a select 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	• Inquired of management if processes to monitor and remediate known security vulnerabilities on the Azure platform are in place.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	been 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 select sample of Azure platform components, obtained and inspected scan results to ascertain the components were monitored for security vulnerabilities. Further, ascertained that identified security vulnerabilities were remediated.	
VM - 7	Procedures to configure and monitor network devices in the scope boundary, and resolve issues, have been established.	• Inquired of the Networking team 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. • For a select sample of network devices in the scope boundary, obtained and inspected device configurations to ascertain that the devices were in compliance with established standards. For devices that were not in compliance, ascertained that issues were investigated and resolved.	No exceptions noted.
VM - 8	Penetration testing of critical infrastructure components is performed at least annually based on documented Penetration testing procedures	• Inquired of the management regarding the procedures established to perform penetration testing on the Azure environment.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	and findings are documented, tracked, and remediated.	• 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 – Findings of the penetration testing were 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.	• Inquired of the Networking team to ascertain that network devices in the scope boundary are configured to log and collect security events, and monitored for compliance. • For a select 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 select sample of 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 - 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 the 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.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		• For a select 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.	
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. • For sampled network devices, selected a sample of vulnerabilities and their corresponding remediation procedures 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 if information security incidents are managed through designated responsibilities and documented procedures. • Obtained and inspected information security incident management procedures and ascertained that roles and responsibilities for escalation and notification to specialist groups during a security incident were established and communicated.	No exceptions noted.
IM - 2	Events, thresholds, and metrics have been defined and configured to detect incidents and alert the associated Operations team.	• Inquired 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.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		• For a select sample of platform components, ascertained that automated notifications were received upon the occurrence of an event meeting the configured specifications.	
IM - 3	The Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures.	• Inquired about the procedures for 24x7 monitoring and handling of incidents. • Identified the population of incidents (all severities) in the examination period and obtained and inspected the incident tickets for a select 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. • 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 if a post-mortem is performed for customer impacting severity 0 and 1 incidents and a formal report is submitted for management review. • Performed a walkthrough with the control owner to understand the mechanisms 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.
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	• Inquired of the Cyber Defense Operations Center (CDOC) team if information security review report is presented to Cloud + AI management on a quarterly basis.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	systemic issues are submitted to executive leadership for review.	• Obtained and inspected the quarterly report 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.	
IM - 6	The Cyber Defense Operations Center (CDOC) team performs annual tests on the security incident response procedures.	• Inquired of the Cyber Defense Operations Center (CDOC) team 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 CDOC 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 the Datacenter Management team if access levels are established and if physical access to the datacenter is restricted to authorized personnel. • Inspected the datacenter SOP and ascertained that procedures were in place to restrict physical access to the datacenter for employees, vendors, contractors, and visitors. Inquired of the management regarding the review and communication of the procedures. • Performed a walkthrough at a sample of in-scope datacenters and observed the following: – Tour groups / visitor / temporary badges were issued after verification of identity and retention of government issued ID	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		– Tour groups / visitors were escorted by designated personnel with escort privileges – Visitor access logs were maintained – Personnel wear badges that were visible for examination upon entry and while working in the facility • 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.	
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.	• Inquired of the Datacenter Management team that security verification and check-in procedures are established for personnel requiring temporary access to the interior datacenters. • Performed walkthroughs of a selection of datacenters and observed temporary / visitor badges were issued upon verification of identity with designated staff escorting authorized persons and visitor access logs were maintained. • Selected a sample of temporary badges that were issued for the datacenters selected for walkthrough and tested that user's identity was verified prior to issuance of the badge. • Selected a sample of temporary badges that were returned for the datacenters selected for walkthrough and tested that the badge access was deactivated upon return.	No exceptions noted.
PE - 3	Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team.	• Inquired of the Datacenter Management team if physical access to datacenters is reviewed and verified quarterly.	**Exception Noted:** For 1 of the 6 sampled datacenter user access reviews

Control ID	Control Activity	Test Procedures	Results of Tests
		• Inspected Datacenter Services (DCS) operating procedures and ascertained that quarterly access review procedures were documented. • Selected a sample of quarterly access reviews for a selection of in-scope datacenters and ascertained that the reviews were performed according to the documented procedures. • For a sample of access modifications needed based on the performance of selected reviews, inspected completed access changes.	from the portion of the period, April 1, 2019 through December 31, 2019, an incomplete listing of access was reviewed during the performance of the control. D&T sampled 10 datacenter user access reviews subsequent to December 31, 2019, and no additional exceptions were 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 the Datacenter Management team if physical access mechanisms to restrict access to authorized individuals are in place. • Performed a walkthrough at a sample of datacenters and 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). • Attempted to access a restricted area within the facility during the walkthrough without appropriate level of access and noted that access was denied.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
PE - 5	The datacenter facility is monitored 24x7 by security personnel.	• Inquired of the Datacenter Management team if security personnel monitor the datacenter premises through a video surveillance system 24 hours a day, 7 days a week, as well as through physical walkthroughs of the facility. • Observed security personnel as well as video surveillance systems at a sample of datacenters during the walkthrough and tested 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 tested that the tapes were retained according to the documented operating procedures.	No exceptions noted.
PE - 6	Datacenter Management team maintains and tests datacenter-managed environmental equipment within the facility according to documented policy and maintenance procedures.	• Inquired of the Datacenter Management team 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. • Performed a walkthrough at a sample of datacenters and observed that the critical environment was being monitored to maintain a consistent level of protection. • Inspected maintenance and testing records for a sample of on-site environmental equipment.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
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.	• Inquired of the Datacenter Management team if environmental controls are implemented to protect systems inside the datacenters. • Performed a walkthrough at a sample of datacenters and observed if the 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.
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 the physical security management team 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 the service teams to understand the mechanisms implemented to allow customers to configure access or traffic restrictions. • Re-performed the control for a select 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	• Inquired of the service teams regarding controls in place to ascertain the following requirements:	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	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.	– 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 • Re-performed the control for a select sample of services through various scenarios such as: – Providing sample weak passwords – 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 the service teams to understand the segregation controls implemented to restrict unauthorized access to other customer tenants. • Re-performed the control for a select 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 the service teams to understand the controls implemented to protect customer confidential data stored within the service. • Re-performed the control for a select sample of services to ascertain that customer confidential data stored within the service was protected.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
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.	• Inquired of the service teams 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. • Re-performed 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.	No exceptions noted.
LA - 7	Quotas on Azure services are enforced as configured by the service administrators to protect against availability related issues.	• Inquired of the service teams to understand the mechanisms in place that allow customers to implement quotas on the service. • Re-performed the control for a select 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 the service teams 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 select 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.

Control ID	Control Activity	Test Procedures	Results of Tests
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 the service team 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. • Re-performed the control using a subscription and ascertained that the service was initialized based on customer configured templates. • Re-performed the control to ascertain that the distribution of the system resource created within a resource group can be monitored and controlled by customers.	No exceptions noted.
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 the service teams regarding monitoring of errors generated during the job execution and actions taken based on the job settings defined by the customer administrator. • Re-performed the control for a select 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	• Inquired of the service team 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	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	identifiable information during the password reset. Azure Active Directory 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.	– 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 Azure Active Directory (Azure AD) password policy requirements • Re-performed the control and obtained sample SMS and email OTPs to ascertain that the characters in the SMS and email were random. • Re-performed 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. • Re-performed 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. • Re-performed 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.	

Control ID	Control Activity	Test Procedures	Results of Tests
ED - 1	Production servers that reside in edge locations are encrypted at the drive level.	• Inquired of the Front Door team to gain an understanding of the encryption mechanism present at the drive level on production servers. • For a select 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 the Front Door team to understand the mechanism for detecting and alerting unauthorized physical access to production servers. • For a select 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.
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 the Front Door team to understand the configuration settings used to disable unused IO ports on production servers. • Obtained and inspected the configuration files for a select 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.	• Inquired of the Business Continuity group to understand the processes in place for developing and maintaining business continuity plans. • Obtained and inspected the business continuity plans and business impact analysis for a sample of components showing that an RTO / RPO was defined and that there were plans in place for each component.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	Plans are reviewed on an annual basis, at a minimum.	• Obtained and inspected the review and approval of the RTO / RPO and BCP.	
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 the Business Continuity group to understand the processes in place for developing and maintaining business continuity plans. • Obtained and inspected the Business Continuity and Disaster Recovery (BC / DR) Standard Operating Procedure to ascertain that it included the defined information security and availability requirements. • Obtained and inspected the overall business continuity plan to ascertain that it included the defined information security and availability requirements.	No exceptions noted.
BC - 4	The BCP team conducts testing of the business continuity and disaster recovery plans 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.	• Inquired of the Business Continuity group to understand the process in place for testing the business continuity / disaster recovery (BC / DR) plans. • For a sample of Azure services, obtained and inspected the BC / DR testing plan and results documents, including follow-up documentation for any issues identified and ascertained that they were established, reviewed and tested at least annually.	No exceptions noted.
BC - 5	Risk assessments are conducted to identify and assess business continuity risks related to Azure services.	• Inquired of Azure Compliance to understand the processes in place for identifying and assessing the business continuity risks related to Azure services. • Obtained and inspected the Business Impact Analysis (BIA) and the Business Continuity Risk Assessment to identify that, for a selection of components, the business impact analysis was completed and impacts were assessed for critical	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		services based on revenue and operational considerations.	
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.	• Inquired of the 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. • Obtained and inspected meeting notes and scorecards, as applicable, to ascertain that SLA monitoring was being performed.	No exceptions noted.
BC - 7	Datacenter Business Continuity Management (BCM) program to respond to Microsoft's Enterprise Business Continuance Initiative has been implemented and includes documented procedures for performing a Business Impact Analysis, establishing Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), 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	• Inquired of Business Continuity Management team to understand the requirements established by Microsoft's Enterprise Business Continuity Management (EBCM) Program. • Obtained and inspected a selection of Datacenter BCM program documents and ascertained that Datacenter BCM program adhered to BCM PMO standards, methods, policies and metrics.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	vulnerabilities and respond to a major disruptive events.		
BC - 8	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 the Business Continuity Management team if datacenters exercise, test and maintain Business Continuity Plans (BCPs) at least once a year. • Obtained and inspected the Datacenter Business Continuity Plan Overview and Procedures and ascertained that recovery strategies and procedures for resumption of critical business processes were documented and that the process for exercising and testing of the plans for continuity and resumption of critical business processes were established. • Obtained and inspected the tests performed for the select sample of datacenters and ascertained that business continuity plans were tested on an annual basis.	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 the Business Continuity Management team if a resiliency assessment specific to the operations of datacenters is conducted and operated by management on an annual basis or prior to proposed significant changes. • Selected a sample and requested the resiliency assessment and ascertained that: – The Cloud Operations & Innovation (CO+I) Team assigned risk ownership – Development of risk treatment plans to address risks were specific to datacenter operations	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 the service team to understand the procedures established to monitor capacity for network devices. • Obtained and inspected the UAL NetSim Report for sampled months to ascertain that network is monitored to ensure availability and address capacity issues on a monthly basis.	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 Azure service teams 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 Azure service teams 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 Azure service teams to understand mechanisms to perform input validation to restrict unauthorized access or non-permissible requests. • Re-performed the control to ascertain that invalid input provided by the user generated error messages for non-permissible requests.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
PI - 4	Microsoft Azure segregates and appropriately provisions the services based on request from customer through the portal / API.	• Inquired of Azure service teams to understand mechanisms to perform request segregation and provision requested services to user accounts. • Re-performed the control to ascertain that service requests were segregated and provisioned based on subscription ID and other request parameters.	No exceptions noted.
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 the management regarding the procedures related to the identification and classification of key information or data. • 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 determine that it aligned with the approved definition criteria in the SOP.	No exceptions noted.
SOC2 - 2	Azure services maintain an inventory of key information assets. Procedures to review the inventory on a monthly basis are established.	• Inquired of the management on the process for maintaining and reviewing the inventory of key information or data. • For a sample of months, sampled services and obtained and inspected asset review completion records within the inventory management tool showing monthly review of key information assets. Additionally, obtained email communications to ascertain that changes, if any, were made per the review performed.	No exceptions noted.
SOC2 - 3	Datacenter team controls the delivery and removal of information system components through tickets on the Global	• Inquired of the management to gain an understanding of the process for delivery and removal of assets from datacenters.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	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.	• Obtained the population of transports (both delivery and removal) performed during the examination period, and judgmentally selected sample transports. • For the select sample, obtained and inspected associated evidence (such as tickets, certificates) to ascertain that proper authorization was obtained prior to asset delivery and / or removal.	
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 the 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. • Identified the population of incidents in the examination period and obtained the Incident Management (IcM) tickets for a select 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.	• Inquired of the management regarding the process for maintaining and communicating confidentiality and related security obligations for customer data to customers. • Inspected Microsoft Trust Center to ascertain that confidentiality and related security obligations were maintained and communicated to customers.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		• Obtained and inspected changes documented in Microsoft Trust Center to ascertain that changes related to the confidentiality and related security obligations were communicated to customers.	
SOC2 - 8	Azure maintains and distributes an accurate system description to authorized users.	• Inquired of the 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 the 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. • Performed a walkthrough of a sample incident ticket to verify 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.

Control ID	Control Activity	Test Procedures	Results of Tests
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 Microsoft Online Services Terms, Microsoft Online Subscription Agreement, Azure service Privacy Statement and Technical Overview of the Security Features in Azure service.	• Inquired of the 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 / agree to prior to gaining access, and ascertained that they addressed identified security requirements. • Created a test subscription to ascertain that agreements were required to be signed prior to subscription creation.	No exceptions noted.
SOC2 - 11	Microsoft has defined disciplinary actions for employees and contingent staff that commit a security breach or violate Microsoft Security Policy.	• Inquired of the HR team 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	• Inquired of the Human Resources (HR) team if procedures were established to perform background checks on new or transferred Microsoft personnel before they were granted access to data and assets.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	screening is conducted in accordance with customer specific requirements, for employees with access to applicable data.	• 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 "HeadTrax" from the examination period. Selected a sample of new hires to ascertain that background checks were performed prior to employment, and additional screening was conducted in case access was being granted to critical data / applications.	
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.	• Inquired of the Human Resources (HR) team if Non-Disclosure Agreements (NDAs), that include asset protection and return responsibilities, were signed as a part of the onboarding process. • Inspected a sample NDA to ascertain that the agreement included requirements for asset protection, and asset return upon termination of employment. • Obtained the total population of new hires from "HeadTrax" 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.	No exceptions noted.
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 the management regarding the process for requiring employees, contractors, and third-party users to follow established security policies and procedures. • Inquired of the management on the process for identifying and reviewing requirements that were	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		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.	
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.	• Inquired of the 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 select 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.
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 the 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.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		• Obtained and inspected policy, procedure, and agreement documents to ascertain that they included relevant and current statutory, regulatory, and contractual requirements.	
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 the 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 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	• Inquired of the management regarding the process for performing the Information Security Management System (ISMS) review. • Inquired of the management regarding the process for planning and performing audit activities. • Obtained and inspected the latest ISMS review to ascertain that the review was performed and results 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.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	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.	• Inquired of the 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) 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 the management on the annual risk assessment process and how security, continuity and operational risks are addressed. • Obtained the risk management procedure to ascertain that procedures for identifying, assessing and monitoring risks were established. • Obtained and inspected the risk assessment reports for the latest risk assessment performed by Microsoft Azure management for a sample of services, to ascertain that threats to security were identified and the risk from these threats was assessed.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
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 the management regarding the annual independent audit process. • 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.
CCM - 1	Microsoft Azure has established policies for mobile computing devices to meet appropriate security practices prior to being connected to the production environment.	• Inquired of the 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.
CCM - 2	Microsoft Azure has included a clear desk and clear screen policy which users are provided as a part of onboarding.	• Inquired of the management that a documented clear desk and clear screen policy exists. • Obtained and inspected Microsoft Azure's clear desk and clear screen policy and ascertained that it addressed applicable information security requirements. Additionally, ascertained that the	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		policy was communicated to users as a part of the on-boarding process.	
CCM - 3	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 the 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 to ascertain that procedures for collection, protection, and retention of audit logs were documented. • Obtained security groups and membership to ascertain that access to audit logs were restricted to individuals authorized by the service team and audit logs were retained as per the documented procedures. • Obtained and inspected the configuration setting to ascertain timely deletion of logs after the retention period.	No exceptions noted.
CCM - 4	Microsoft Azure components are configured to use Coordinated Universal Time (UTC) time and the clocks are synchronized with the domain controller server.	• Inquired of the management regarding the procedures in place for time synchronization across the various Azure components. Additionally, inquired if Azure uses a centralized synchronized time-service protocol (such as Network Time Protocol (NTP)), which synchronizes with UTC, to ascertain that systems, including domain controllers have a common time reference. • Observed mechanisms used by Azure including configurations to sync time and clocks across the Azure components, including domain controllers, to UTC.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
CCM - 5	Microsoft Capacity Management team projects future capacity requirements based on internal operational reports, revenue forecasts and inputs from internal component teams.	• Inquired regarding the capacity planning process and process to review the capacity model with the management. • Obtained and inspected the monthly capacity planning review decks pertaining to capacity planning to ascertain that the necessary parameters were reviewed and considered during the capacity planning.	No exceptions noted.
CCM - 6	Azure has published a standard set of APIs with an ecosystem of tools and libraries on the Azure Portal.	• Inquired of the management regarding the list of Application Programming Interfaces (APIs) that Azure offers to customers. • Inspected the 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 like REST etc.	No exceptions noted.
CCM - 9	Microsoft Azure has established forensic procedures to support potential legal action after an information security incident.	• Inquired of the management regarding the forensic procedures in place for preservation and presentation of evidence, to support potential legal action after an information security incident. • Obtained and inspected forensic procedures and ascertained that procedures and methodologies for gathering and securing evidences were defined.	No exceptions noted.
C5 - 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	• Inquired of the management regarding the process for establishing, maintaining, updating and reviewing Standard Operating Procedures. • Obtained the latest Standard Operating Procedures (SOPs) to ascertain they included appropriate	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	reviewed and approved annually by appropriate management.	attributes, and were reviewed and approved in a timely manner.	
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 the 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 - 5	Customer metadata is collected, retained, and removed based on the documented procedures.	• Inquired of the management to understand the process regarding customer metadata collection, retention and deletion. • Inspected configurations to ascertain that mechanisms existed for collecting, retaining and deleting customer metadata 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 the management to understand the process and mechanism in place for enforcing authenticated access to the logging and monitoring infrastructure. • Through observation and inspection of security configurations, ascertained that mechanisms existed for logging servers to establish an authenticated connection with the logging infrastructure and that it takes place over an encrypted channel. • Through inspection ascertained that only authorized individuals were part of the security group that had access to logging and monitoring infrastructure.	No exceptions noted.

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 the 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.
ELC - 1	Microsoft's values are accessible to employees via the Values SharePoint site and are updated as necessary by management.	• Inquired of the management regarding Microsoft's values and the process for updating and making them accessible to employees. • Observed the Values SharePoint site and ascertained that Microsoft's values are defined, updated as needed, and published to employees.	No exceptions noted.
ELC - 2	Microsoft Office of Legal Compliance (OLC) 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. OLC 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 the Microsoft Office of Legal Compliance (OLC) team 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 select 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 Microsoft Office of Legal Compliance (OLC) team regarding the mechanisms (email, phone, fax, website) that permit reporting of issues related to Business Conduct. • Accessed each communication mechanism to ascertain that the mechanisms were available and functioning.	No exceptions noted.
ELC - 4	The Audit Committee (AC) reviews its Charter and Responsibilities 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 the members of the Audit Committee (AC) to gain an understanding of the Charter and Responsibilities of the Audit Committee and its annual review process. • Obtained and inspected the agenda or meeting minutes to ascertain the annual review of Audit Committee's Charter and Responsibilities Calendar. • Inspected the investor relations website to ascertain that the Audit Committee's Charter and Responsibilities Calendar was published on the website. • Obtained evidence (e.g., meeting invite, meeting minutes) to ascertain quarterly meetings between AC and internal / external auditors.	No exceptions noted.
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	• Inquired of the management to gain an understanding of the Internal Audit Charter and the scope and frequency of assurance activities performed by Internal Audit. • Obtained and inspected the Internal Audit Charter and ascertained that the Charter directs the services of the Internal Audit.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	of assurance activities is based on an annual risk assessment.	• Obtained and inspected the Internal Audit plan and ascertained that the assurance activities are based on an annual risk assessment.	
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.	• Inquired of the management regarding the process for: – Citing expectations from outsourced providers to achieve specific deliverables – Training outsourced providers on Microsoft's supplier code of conduct • Obtained and inspected Microsoft's SOW template to ascertain that it cited outsourced providers' role and accountability in achieving specific deliverables. • Inspected the supplier procurement website to ascertain that Microsoft's supplier code of conduct is available and accessible to all outsourced providers. • Observed during the supplier access provisioning process that completion of the supplier code of conduct training is required.	No exceptions noted.
ELC - 7	Employees hold periodic "connects" with their managers to validate they are on the expected career path and facilitate greater collaboration. Employees also review their performance against their documented deliverables (priorities) and discuss the results with their managers.	• Inquired of the Human Resources (HR) team that periodic connects take place at least annually, where employee's commitments are evaluated by his or her manager. • Obtained and inspected the documentation of a sample periodic connect to ascertain that it included an evaluation of the employee's performance against the documented deliverables (priorities). • For a select sample of employees, obtained evidence of occurrence of periodic connects to ascertain that the connects occurred at least annually.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
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 the members of the Compensation Committee to gain an understanding of the process for planning of executive officer development and corporate succession plans for the CEO and other executive officers. • Obtained and inspected the agenda or meeting minutes to ascertain the annual discussion of the succession plans. • Inspected the Compensation Committee Charter on the investor relations website to ascertain that the Compensation Committee's responsibility included reviewing the succession plan for CEO and other executive officers, on an annual basis.	No exceptions noted.
ELC - 9	The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management.	• Inquired of the Enterprise Risk Management (ERM) team on the ERM risk assessment process and how risks are identified and managed. • Obtained and inspected the agenda or meeting minutes to ascertain that the ERM risk assessment results are reviewed bi-annually and presented to the Board of Directors for review and consideration of the changes.	No exceptions noted.

Section V: Supplemental Information Provided by Microsoft

Section V: Supplemental Information Provided by 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 Microsoft Trust Center.

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 Online Services Terms (OST) http://aka.ms/Online-Services-Terms:

- 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 Secure Development Lifecycle - SDL is Microsoft's security assurance process that is employed during the development of Azure: http://www.microsoft.com/security/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: http://www.microsoft.com/security/msrc/default.aspx or via email to secure@microsoft.com

Management's Response to Exceptions Noted

The table below contains Management's response to the exceptions identified in Section IV - Information Provided by Independent Service Auditor Except for Control Activities and Criteria Mappings above.

Control ID	Control Activity	Exception Noted	Management Response
OA - 15	Passwords used to access Azure network devices are restricted to authorized individuals based on job responsibilities and changed on a periodic basis.	Exceptions were identified in the period previous to the current examination period. Evidence related to password rotation was not retained and not available for inspection to corroborate that the passwords were changed on a periodic basis. Per inquiry of management, remediation for this control was in progress from April 1, 2019 through June 30, 2019. D&T sampled 26 samples subsequent to June 30, 2019, and no additional exceptions were noted.	Management committed to providing a long-term solution to automate password rotation for network devices across all cloud instances. The automated solution was rolled out across the Public and Government cloud instances. Per testing performed by D&T subsequent to June 30, 2019, no additional exceptions were identified. Management considers this control to be remediated subsequent to June 30, 2019.
PE - 3	Physical access to the datacenter is reviewed quarterly and verified	For 1 of the 6 sampled datacenter user access reviews from the portion of the period, April 1, 2019	The exception was due to an incorrect report being generated to facilitate the user access review at a new site. As a result, 3 users with access to the site

Control ID	Control Activity	Exception Noted	Management Response
	by the Datacenter Management team.	through December 31, 2019, an incomplete listing of access was reviewed during the performance of the control. D&T sampled 10 datacenter user access reviews subsequent to December 31, 2019, and no additional exceptions were noted.	were missed in the review; however, they were deemed appropriate based on their job responsibilities and access should continue. In addition, the 3 users' access are limited and do not have access to the server rooms. Additional training has been implemented to ensure proper procedures are followed per the operating procedures. Per testing performed by D&T subsequent to December 31, 2019, no additional exceptions were identified. Management considers this control to be remediated subsequent to December 31, 2019.

Dynamics Controls to Azure Controls Mapping

For the consolidation of the Microsoft Dynamics 365 controls into the Microsoft Azure SOC controls, the table below contains a mapping of the controls formerly tested within the Microsoft - Dynamics 365 SOC 2 report to the Microsoft Azure controls tested within this report. Users of this report can use this table as a reference for the previous Microsoft Dynamics 365 controls to the controls in this report.

Microsoft Dynamics 365 Control Activity	Azure Control Activity
CA-1. Senior Management, as part of its annual planning process, considers its commitments and requirements for security, availability, processing integrity and confidentiality.	**IS - 4.** An information security education and awareness program that includes policy training and periodic security updates for Azure personnel has been established.
CA-2. A Dynamics 365 security virtual team has been defined and is responsible for Security issues within the Dynamics 365 environment. Service teams have operations personnel who are responsible for system operation, monitoring and service availability.	**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.
CA-3. A Dynamics governance, compliance, and risk team has been defined and is responsible for security and availability controls within the Dynamics 365 environment.	**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.

Microsoft Dynamics 365 Control Activity	Azure Control Activity
	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. **BC - 5.** Risk assessments are conducted to identify and assess business continuity risks related to Azure services.
CA-4. Employees hold periodic "connects" with their managers to validate they are on the expected career path and facilitate greater collaboration. They also review their performance against their documented deliverables (priorities) and discuss the results with their managers.	**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.
CA-5. As needed, the Governance, Risk, and Compliance team updates the data flows and service offerings of Dynamics 365 and the individuals that act as point of contact for each service offering.	**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.
CA-6. As part of its major system release planning process, Dynamics 365 considers its commitments and requirements to security, availability, processing integrity and confidentiality.	**SDL - 7.** The SDL review for each service with a major release is performed and completed on a semi-annual basis, and signed off on by designated owners.
CA-7. Candidates for open positions go through an interview process with multiple interviewers. The interviewer feedback is documented in the internal tool RecWeb. The interviewers provide competency and technical/functional based assessments of candidates in a text box and enter a HIRE or NO HIRE recommendation – which is required.	**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. **IS - 4.** An information security education and awareness program that includes policy training and periodic security updates for Azure personnel has been established.
CA-8. Microsoft Office of Legal Compliance (OLC) updates the Standards of Business Conduct as necessary and the Code is made available to all employees at http://businessconduct. The SBC reflects Microsoft continued commitment to ethical business practices and regulatory compliance. OLC provides an annual Standards of Business Conduct training course that is mandatory for all employees. Employees who do	**ELC - 2.** Microsoft Office of Legal Compliance (OLC) 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. OLC provides an annual Standards of Business Conduct training course that is mandatory for all employees.

Microsoft Dynamics 365 Control Activity	Azure Control Activity
not complete the training on time are tracked and followed up with appropriately.	Employees who do not complete the training on time are tracked and followed up with appropriately.
CA-9. The Dynamics 365 group works with Microsoft Human Resources and vendor companies to perform a background check on new or transferred U.S. personnel before they are granted access to the Microsoft Online Services production assets containing customer data.	**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.
CA-10. Dynamics 365 system information regarding design and operation is available to all users on the internet through the Microsoft customer facing portals.	**SOC2 - 8.** Azure maintains and distributes an accurate system description to authorized users.
CA-11. Customers that request the annual SOC report for Dynamics 365 get a listing of complementary user entity controls (CUEC) outlining external users' responsibilities for system operation.	**SOC2 - 7.** Azure maintains and communicates the confidentiality and related security obligations for customer data via the Microsoft Trust Center.
CA-12. On an annual basis Standard Operating Procedures are updated to reflect changes made to the Dynamics 365 processes. Standard Operating Procedures are made available to internal system users via the SharePoint.	**IS - 3.** Management has established defined roles and responsibilities to oversee implementation of the Security Policy across Azure.
CA-13. Dynamics 365 communicates its commitments to customers in SLAs. These commitments are distributed internally through documented policies and Standard Operating Procedures.	**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 Microsoft Online Services Terms, Microsoft Online Subscription Agreement, Azure service Privacy Statement and Technical Overview of the Security Features in Azure service.
CA-14. Incident response guides are used by Dynamics 365 personnel for the handling and reporting of security incidents. These guides are stored on Internal SharePoint sites and are updated as needed.	**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.
CA-15. Customers are notified of incidents and changes to the Dynamics 365 environment through email communications to the customer's administrative accounts.	**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.

Microsoft Dynamics 365 Control Activity	Azure Control Activity
CA-16. Customers can report and receive information around security, availability, confidentiality, and processing integrity issues through the Customer Portal and Account Representatives.	**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.
CA-17. Dynamics 365 adheres to corporate Microsoft Security Policy, which is owned by the Microsoft Chief Information Security Officer. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses asset classification (to include data), risk assessment, access control, change control and acceptance, incident response, exceptions, training, and where to go for additional information. The policy is available to all employees on the company's internal portal.	**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.
CA-18. All changes to the Dynamics 365 environment follow documented change management procedures and are tracked in a change management database.	**CM - 1.** Procedures for managing different types of changes to the Azure platform have been documented and communicated.
CA-19. Key stakeholders approve major and minor changes prior to release into production.	**CM - 2.** Key stakeholders approve changes prior to release into production based on documented change management procedures. **CM - 3.** Responsibilities for requesting, approving, and implementing changes to the Azure platform are segregated among designated personnel. **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.
CA-20. Emergency changes to production environment follow the emergency change approval process.	**CM - 11.** Change management processes include established workflows and procedures to address emergency change requests.
CA-21. Microsoft takes a deliberate approach to risk management and annually conducts a risk assessment. The purpose is to identify and prioritize the threats facing Dynamics 365 and prioritize the most preeminent risks based on impact, likelihood, and	**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.

Microsoft Dynamics 365 Control Activity	Azure Control Activity
managements controls. Additionally, clear ownership is established for each risk and its mitigation strategy. This is reviewed annually by Dynamics 365 management with ownership assigned out to individual teams and their management.	
CA-22. Effectiveness of existing controls are assessed internally, through risk assessments, vulnerability scanning, and other methods, as well as by third parties on an annual basis. Findings are addressed with corrective actions, which are tracked to support that they are completed in a timely manner.	**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.
CA-23. 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 - 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.
CA-24. Identity of Microsoft internal users is authenticated to Dynamics 365. The use of passwords includes periodic password change and password complexity.	**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.
CA-25. Privileged accounts are reviewed quarterly to determine if the privileged access level is still appropriate. Access is modified based on the results of the reviews.	**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.
CA-26. Access privileges are reviewed at least every six (6) months to determine if access rights are commensurate to the user's job duties. Access is modified as needed based on the results of the reviews.	**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.

Microsoft Dynamics 365 Control Activity	Azure Control Activity
CA-27. Authentication over an encrypted Remote Desktop Connection is used for access to the production environment.	**OA - 8.** Authentication over an encrypted Remote Desktop Connection is used for administrator access to the production environment.
CA-28. When users no longer require access or upon termination the user access privileges are revoked in a timely manner.	**OA - 3.** Procedures to automatically disable Active Directory (AD) accounts and manually remove any non-AD accounts upon user's leave date are in place.
CA-29. Each Dynamics 365 customer's data is segregated either logically or physically from other Dynamics 365 customer data.	**DS - 16.** Each Online Service's customer's data is segregated from other Online Services' customers' data, either logically or physically.
CA-30. Processes and procedures have been established to report security incidents to the Security team. Security incidents are identified and tracked in an incident tracking system.	**IM - 2.** Events, thresholds, and metrics have been defined and configured to detect incidents and alert the associated Operations team.
CA-31. Security events escalated to Security team are reviewed by Security Incident Response Team and action is taken in accordance with the established incident response program procedures.	**IM - 3.** The Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures.
CA-32. Production assets are scanned for vulnerabilities and results are reviewed and remediation is tracked through closure.	**VM - 4.** Procedures to investigate and respond to malicious events detected by the Azure monitoring system in a timely manner have been established.
CA-33. A patch management process exists to confirm that operating system level vulnerabilities are remediated in a timely manner.	**VM - 5.** Procedures to evaluate and implement Microsoft-released patches to Service components have been established.
CA-34. Production servers are scanned to test patch compliance on a quarterly basis.	**VM - 6.** Procedures to monitor the Azure platform components for known security vulnerabilities have been established. Identified security vulnerabilities are remediated.
CA-35. New system development and changes follow an approved development approach modeled after the Microsoft corporate Software Development Life Cycle.	**SDL - 1.** Development of new features and major changes to the Azure platform follow a defined approach based on the Microsoft Secure Development Lifecycle (SDL) methodology.
CA-36. System development requirements or changes are documented and approved by key stakeholders.	**SDL - 2.** Applicable operational security and internal control requirements are documented and approved for major releases prior to production deployment. **SDL - 4.** New features and major changes are developed and tested in separate environments prior to production implementation. Production

Microsoft Dynamics 365 Control Activity	Azure Control Activity
	data is not replicated in test or development environments.
CA-37. Key stakeholders provide a Go/No-go sign-off prior to deploying the releases in production indicating their approval of the production readiness of the tested code.	**SDL - 3.** Responsibilities for submitting and approving production deployments are segregated within the Azure teams.
CA-38. Production releases undergo security review such as Security Development Lifecycle (SDL) prior to their release into production environment per the criteria defined.	**SDL - 7.** The SDL review for each service with a major release is performed and completed on a semi-annual basis, and signed off on by designated owners.
CA-39. Dynamics 365 has on-call personnel who respond to potential security and availability incidents. If an incident is assigned a high enough severity, the manager on shift will work with the Dynamics 365 team to support that the appropriate contingency plan is followed through to resolution.	**IM - 3.** The Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures.
CA-40. Procedures have been established for back-up and restoration. Back-up restoration is defined and carried out according to procedures.	**DS - 9.** Backup restoration procedures are defined and backup data integrity checks are performed through standard restoration activities.
CA-41. Backups of production data are performed according to the backup schedule.	**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.
CA-42. Customer data is replicated to a geographically separate location.	**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.
CA-43. Processing capacity and availability are monitored by Service teams.	**VM - 12.** The availability of Azure services is monitored through third-party and internal tools, and the status is communicated through a Service Dashboard.
CA-44. Dynamics 365 management reviews capacity and availability on a monthly basis. Any issues with or changes to capacity and availability are tracked to resolution.	**CCM - 5.** Microsoft Capacity Management team projects future capacity requirements based on internal operational reports, revenue forecasts and inputs from internal component teams.

Microsoft Dynamics 365 Control Activity	Azure Control Activity
CA-45. Each Service team conducts regular failover tests to determine they can meet Recovery Time Objectives.	**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 - 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.
CA-46 - Based on meetings with the CELA and other Microsoft groups, the Dynamics 365 Governance, Risk, and Compliance team will update the control framework to meet regulatory, industry, or technology changes.	**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.
CA-47 - Dynamics 365 monitors its dependencies on third parties through obtaining and evaluating attestation reports when available.	**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.
CA-48 - Data in motion is encrypted when transmitting data between the customer and the data center.	**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.
CA-52. Azure-managed network devices are configured to log and collect security events, and monitored for compliance with established security standards.	**VM - 9.** Network devices in the scope boundary are configured to log and collect security events, and monitored for compliance with established security standards.

Microsoft Dynamics 365 Control Activity	Azure Control Activity
CA-53 - Data at rest within the Dynamics 365 environments is encrypted per policy.	**DS - 13.** Production data on backup media is encrypted.
CA-54 - Customer content is retained and deleted after termination of Dynamics 365 subscriptions per agreed upon commitments with the customer in the contract and Service Licensing Agreements.	**DS - 15.** Customer data is retained and removed per the defined terms within the Microsoft Online Services Terms (OST), when a customer's subscription expires, or is terminated.
C5-OIS-1. 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 - 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.
C5-HR-1. 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 - 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-HR-2. Microsoft has defined disciplinary actions for employees and contingent staff that commit a security breach or violate Microsoft Security Policy.	**SOC2 - 11.** Microsoft has defined disciplinary actions for employees and contingent staff that commit a security breach or violate Microsoft Security Policy.
C5-HR-3. Personnel operating the Dynamics 365 Germany Sovereign Cloud are required to complete security trainings on an annual basis. Evidence of training completion is documented.	**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. **IS - 4.** An information security education and awareness program that includes policy training and periodic security updates for Azure personnel has been established.
C5-AM-1. Microsoft Dynamics 365 utilizes an asset management system to identify and inventory assets. The assets are assigned owners, classified, labeled and information entered into the asset management system is validated.	**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.

Microsoft Dynamics 365 Control Activity	Azure Control Activity
	SOC2 - 2. Azure services maintain an inventory of key information assets. Procedures to review the inventory on a monthly basis are established.
C5-RB-1. Microsoft Dynamics 365 utilizes anti-virus protection and repair programs to protect against malware.	**VM - 1.** Azure platform components are configured to log and collect security events. **VM - 3.** A monitoring system to monitor the Azure platform for potential malicious activity and intrusion past service trust boundaries has been implemented.
C5-RB-2. Microsoft Dynamics 365 conducts penetration testing on an annual basis. The tests are carried out according to documented test methods. The results of the penetration testing are assessed and documented.	**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.
C5-RB-3. Microsoft Dynamics 365 servers are hardened according to generally established and accepted industry standards. The hardening standards are documented and retained in a SharePoint site.	**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.
C5-PI-1. Microsoft Dynamics 365 utilizes tools and processes to identify input and output interfaces of different components used for providing services to customers.	**PI - 3.** Microsoft Azure performs input validation to restrict any non-permissible requests to the API.
C5-PI-2. Customer data is accessible within agreed upon services in data formats compatible with providing those services.	**SOC2 - 28.** Customer data is accessible within agreed upon services in data formats compatible with providing those services.
C5-PI-3. Dynamics 365 has processes in place to conduct backups and perform restores of organization databases after customer subscriptions end.	**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.

Microsoft Dynamics 365 Control Activity	Azure Control Activity
C5-PI-4. Dynamics 365 has processes in place to retain and delete customer information according to the defined Online Service Terms.	**DS - 15.** Customer data is retained and removed per the defined terms within the Microsoft Online Services Terms (OST), when a customer's subscription expires, or is terminated.
C5-DLL-1. Microsoft Dynamics 365 conducts weekly reviews of third-party KPIs that support the Germany sovereign cloud.	**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.
C5-BCM-1. Microsoft Dynamics 365 has developed a Business Continuity and Disaster Recovery (BC / DR) Standard Operating Procedure and documentation that includes the defined information security, availability, processing integrity and confidentiality requirements.	**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.
C5-BCM-2. Business Continuity Plans (BCP) have been documented and published for critical Dynamics 365 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). Plans are reviewed on an annual basis, at a minimum.	**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.
C5-BCM-3. Disaster Recovery procedures have been established for Dynamics 365 components. The Disaster Recovery procedures are tested on a regular basis.	**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.
C5-BCM-4. The BCP team conducts testing of the Business Continuity and Disaster Recovery plans for critical services, per the defined testing schedule for different loss scenario. Each loss scenario is tested at least annually. Issues identified during testing are resolved during the exercises and plans are updated accordingly.	**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.
C5-BEI-1. 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 - 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.

Microsoft Dynamics 365 Control Activity	Azure Control Activity
C5-IDM-1. A centralized repository is used for managing source code changes to the Dynamics platform. Procedures are established to authorize Dynamics personnel based on their role to submit source code changes.	**SDL - 5.** A centralized repository for managing source code changes to the Azure platform is used. Procedures to authorize Azure personnel to submit source code changes based on their role, are established.

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 configuring trust and claim rules within Access Control Service.
- Customers are responsible for ensuring the supervision, management and control for access to key systems hosted in the Azure environment.
- Customers are responsible for verifying the security of patching, and maintaining any third party applications and / or components that they install on the Azure 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 Office 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 utilizing the IAM - Management Admin UX service are responsible for monitoring appropriateness of security group memberships.
- Customers are responsible for implementing appropriate authentication mechanisms and only granting admin access to appropriate individuals to maintain the integrity of their AAD tenant.
- Customers utilizing AAD 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 physically securing the StorSimple device in their premise.
- Customers are responsible for specifying strong cloud encryption key used for encrypting the data from their StorSimple device to the cloud.
- Customers are responsible for providing Internet connectivity for their StorSimple device to communicate with Azure.
- 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.