Microsoft

NOTE: You may not distribute this SOC 2 report for Microsoft Azure to other parties, except where Microsoft Azure is a component of the services you deliver to your customers. In this circumstance, you may distribute this SOC 2 report to current and prospective customers / users of your own services. You must provide recipients of this SOC 2 report written documentation of the function that 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 - Microsoft Azure

(Azure & Azure Government)

Service Organization Controls (SOC) 2 Report

October 1, 2017 - September 30, 2018

Table of contents

Executive Summary

Microsoft Azure	
Scope	Microsoft Azure and Microsoft Datacenters
Period of Examination	October 1, 2017 to September 30, 2018
Applicable Trust Principle(s)	Security, Availability, Processing Integrity, and Confidentiality
Location(s)	• Santa Clara, CA (BY1/2/3/4/21/22) • Phoenix, AZ (PHX20, PHX01) • Des Moines, IA (DM1/2/3, DSM05) • Chicago, IL (CH1/3, CHI20) • San Antonio, TX (SN1/2/3/4/5/6) • Ashburn, VA (BL2/3/5/7) • Boydton, VA (BN1/3/4/6) • Dallas, TX (DAL) • Los Angeles, CA (LAX) • Miami, FL (MIA) • Bristow, VA (BLU) • Reston, VA (BL4/6/30) • Tukwila, WA (TK5) • Quincy, WA (CO1/2, MWH01) • Cheyenne, WY (CYS01/04) • San Jose, CA (SJC31, SJC) • New York, NY (NYC) • Stirling, VA (BL20) • Boston, MA (BOS01) • Toronto, Canada (YTO20, YTO01) • Quebec City, Canada (YQB20) • Queretaro, Mexico (MEX30) • Macquarie Park, Australia (SYD03) • Melbourne, Australia (MEL01) • Durham, United Kingdom (MME20) • Chessington, United Kingdom (LON20) • London, United Kingdom (LON21) • Cardiff, United Kingdom (CWL20) • Manchester, United Kingdom (MAN30) • Dublin, Ireland (DB3/4/5, DUB06/07/20) • Paris, France (PAR02/20/21/22) • Marseille, France (MRS20) • Copenhagen, Denmark (CPH30) • Milan, Italy (MIL30) • Stockholm, Sweden (STO) • Brussels, Belgium (BRU30) • Frankfurt, Germany (FRA) • Hong Kong (HK1/2, HKG20) • New Delhi, India (DEL01) • Mumbai, India (BOM01) • Dighi, India (PNQ01) • Ambattur, India (MAA01) • Osaka, Japan (OSA01/02/20)

Microsoft Azure	
	• Sydney, Australia (SYD21, SYD22) • Canberra, Australia (CBR20, CBR21) • Campinas, Brazil (CPQ01/02) • Fortaleza, Brazil (FOR01) • Rio de Janeiro, Brazil (RIO01) • Sao Paulo, Brazil (GRU) • Santiago, Chile (SCL01) • Humacao, Puerto Rico (PR1) • Vienna, Austria (VIE) • Vantaa, Finland (HEL01) • Athens, Greece (ATH01) • Amsterdam, Netherlands (AM1/2/3, AMS04/05/06/20) • Tokyo, Japan (KAW, TYO01/21/22) • Cyberjaya, Malaysia (KUL01) • Singapore (SG1/2/3, SIN20) • Busan, South Korea (PUS01, PUS20) • Seoul, South Korea (SEL20) • Taipei, Taiwan (TPE30) • Manila, Philippines (MNL30) • Johannesburg, South Africa (JNB02) • Cape Town, South Africa (CPT02)
Subservice Providers	N/A
Opinion Result	Unqualified
Testing Exceptions	3

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

Deloitte.

Deloitte & Touche LLP
925 Fourth Avenue, Suite 3300
Seattle, WA 98104-1126
Tel: +1 206 716 7000
www.deloitte.com

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

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

Scope

We have examined the description of the system of Microsoft Azure and Microsoft datacenters (the "Service Organization" or "Azure") in Section III of this Service Organization Controls Report (the "Report"), related to Azure's in-scope services, for Azure and Azure Government cloud environments[1] for the period October 1, 2017 to September 30, 2018 (the "Description") based on the criteria set forth in the American Institute of Certified Public Accountants ("AICPA") DC section 200A*, 2015 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 described therein to meet the criteria for the security, availability, processing integrity, and confidentiality principles ("applicable trust services criteria")[2] set forth in the 2016 edition of TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Principles and Criteria), throughout the period October 1, 2017 to September 30, 2018. We have also examined the suitability of the design and operating effectiveness of controls to meet the requirements set forth in the Cloud Security Alliance's (CSA's) Cloud Controls Matrix (CCM) Version 3.0.1 control specifications ("CCM criteria").

The information included in Section V of the Report, "*Supplemental Information Provided by Microsoft Azure"* in the Report is presented by management of Azure to provide additional information and is not a part of the Description. The information about Service Organization's Azure Compliance, Infrastructure Redundancy and Data Durability, Data Backup and Recovery, Microsoft Azure E.U. Data Protection Directive, Additional Resources, Management's Response to Exceptions Noted, and User Entity Responsibilities, has not been subjected to our procedures applied in the examination of the Description and of the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria and the CCM criteria, and, accordingly, we express no opinion on it.

Service Organization's Responsibilities

In Section II of the Report, Azure has provided an assertion about the fairness of the presentation of the Description based on the description criteria and suitability of design and operating effectiveness of the controls

[1] In-scope services and coverage periods are defined in the *Azure and Azure Government Report Scope Boundary* and *Azure Supporting Infrastructure Services* subsections in Section III of this SOC 2 report. Applicability of the Processing Integrity Trust Services Principle is defined in *the Azure and Azure Government Report Scope Boundary* subsection. In-scope datacenters 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.

described therein to meet the applicable trust services criteria and the CCM criteria. Azure is 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; identifying the risks that would prevent the applicable trust services criteria and the CCM criteria from being met; designing, implementing, and documenting controls to meet the applicable trust services criteria and the CCM criteria; and specifying the controls that meet the applicable trust services criteria and the CCM criteria and stating them in the Description.

Service Auditors' Responsibilities

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

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included procedures that we considered necessary in the circumstances. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the Description is fairly presented based on the description criteria, and the controls were suitably designed and operating effectively to meet the applicable trust services criteria and the CCM criteria throughout the period October 1, 2017 to September 30, 2018. 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 to meet the applicable trust services criteria and the CCM criteria involves:

- Performing procedures to obtain evidence about whether the Description is fairly presented based on the description criteria and the controls were suitably designed and operating effectively to meet the applicable trust services criteria and the CCM criteria throughout the period October 1, 2017 to September 30, 2018.
- Assessing the risks that the Description is not fairly presented and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria and the CCM criteria.
- Testing the operating effectiveness of those controls to provide reasonable assurance that the applicable trust services criteria and the CCM criteria were met.
- Evaluating the overall presentation of the Description.

Inherent Limitations

The Description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to its own particular needs. Because of their nature, controls at a service organization may not always operate effectively to meet the applicable trust services criteria and the CCM criteria. Also, conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria and the CCM criteria, is subject to the risks that the system may change or that controls at a service organization may become ineffective.

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, based on the description criteria and the applicable trust services criteria and the CCM criteria in Section II of the Report:

a. The Description fairly presents the system that was designed and implemented throughout the period October 1, 2017 to September 30, 2018.

b. The controls stated in the Description were suitably designed to provide reasonable assurance that the applicable trust services criteria and the CCM criteria would be met if the controls operated effectively throughout the period October 1, 2017 to September 30, 2018.

c. The controls operated effectively to provide reasonable assurance that the applicable trust services criteria and the CCM criteria were met throughout the period October 1, 2017 to September 30, 2018.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV of the Report, is intended solely for the information and use of Azure, user entities of Azure during some or all of the period October 1, 2017 to September 30, 2018, and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

1. The nature of the service provided by the service organization.
2. How the service organization's system interacts with user entities, subservice organizations, and other parties.
3. Internal control and its limitations.
4. The applicable trust services criteria and the CCM criteria.
5. The risks that may threaten the achievement of the applicable trust services criteria and the CCM criteria, and how controls address those risks.

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

Deloitte & Touche LLP

October 31, 2018

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

Section II: Management's Assertion

We have prepared the description of the system in Section III of Microsoft Azure and Microsoft datacenters (the "Service Organization" or "Azure") throughout the period October 1, 2017 to September 30, 2018[3] (the "period") related to Azure's in-scope services, for Azure and Azure Government cloud environments, based on criteria in items (1)(a)-(b) below, which are the criteria for a description of a service organization's system in DC section 200A, 2015 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, particularly system controls intended to meet the criteria for the security, availability, processing integrity and confidentiality principles ("applicable trust services criteria")[4] set forth in the 2016 edition of TSP section 100A, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Principles and Criteria), and the criteria set forth in the CSA Cloud Control Matrix (CCM) Version 3.0.1 control specifications ("CCM criteria").

Description Criteria

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

1. The description fairly presents the system related to Azure's in-scope services throughout the period October 1, 2017 to September 30, 2018, based on the following description criteria:

   a. The description contains the following information:

      i. The types of services provided.

      ii. The components of the system used to provide the services, which are as follows:

         (a) *Infrastructure.* The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and other telecommunications networks).

         (b) *Software.* The application programs and IT system software that support application programs (operating systems, middleware, and utilities).

         (c) *People.* The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).

         (d) *Procedures.* The automated and manual procedures.

         (e) *Data.* Transaction streams, files, databases, tables, and output used or processed by the system.

[3] In-scope services and coverage periods are defined in the *Azure and Azure Government Report Scope Boundary* and *Azure Supporting Infrastructure Services* subsections in Section III of this SOC 2 report. Applicability of the Processing Integrity Trust Services Principle is defined in the *Azure and Azure Government Report Scope Boundary* subsection. In-scope datacenters 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.

iii. The boundaries or aspects of the system covered by the description.

iv. For any information that is provided to, or received from, subservice organizations or other parties:

(a) How such information is provided or received and the role of the subservice organization or other parties.

(b) The procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

v. The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:

(a) Complementary user-entity controls contemplated in the design of the service organization's system.

(b) When the inclusive method is used to present a subservice organization, controls at the subservice organization.

vi. For those subservice organizations using the carve-out method:

(a) The nature of the services provided by the subservice organization.

(b) Each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria.

vii. Any applicable trust services criteria and CCM criteria that are not addressed by a control at the service organization and the reasons.

viii. Relevant details of changes to the service organization's system during the period covered by the description.

b. The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

2. The controls stated in the description were suitably designed throughout the period to meet the applicable trust services criteria and CCM criteria.

3. The controls stated in the description operated effectively throughout the period to meet the applicable trust services criteria and the CCM criteria.

Section III: Description of Microsoft Azure System

Section III: Description of Microsoft Azure System

Overview of Operations

Business Description

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 and many other 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 Online Services that are in scope for this report.

"Azure", when referenced in this report, comprises "Microsoft Azure", "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 Azure that may be relevant to customers pursuing the security, availability, processing integrity, and confidentiality trust principles. Azure has considered the service-specific characteristics and commitments to determine applicability of the SOC 2 Trust Principles for the in-scope services. Based on the guidance from AICPA, the following are the applicability considerations:

Trust Principle	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
Availability	Addresses risks related to system accessibility for processing, monitoring and maintenance	Applies to the Azure services whose accessibility is advertised or committed by contract
Processing Integrity	Addresses risks related to completeness, accuracy, and timeliness of system / application processing of transactions	Applies to the Azure services 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

Trust Principle	Description	Applicability Considerations
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 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 are in scope for this report:

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[5]			
		Azure	Azure Government	Q4 2017	Q1 2018	Q2 2018	Q3 2018
Microsoft Datacenters							
Microsoft Datacenter and Operations Service		✓	✓	✓	✓	✓	✓
Azure							
Compute	Azure Migrate	✓	-	-	-	✓	✓
	Batch	✓	✓	✓	✓	✓	✓
	Cloud Services	✓	✓	✓	✓	✓	✓
	Functions[6]	✓	✓	✓	✓	✓	✓

[5] Examination Period scope Q4 2017 extends from October 1, 2017 to December 31, 2017.
Examination Period scope Q1 2018 extends from January 1, 2018 to March 31, 2018.
Examination Period scope Q2 2018 extends from April 1, 2018 to June 30, 2018.
Examination Period scope Q3 2018 extends from July 1, 2018 to September 30, 2018.

[6] Examination Period for this service for Azure Government is from January 1, 2018 to September 30, 2018.

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[5]			
		Azure	Azure Government	Q4 2017	Q1 2018	Q2 2018	Q3 2018
	Service Fabric	✓	✓	✓	✓	✓	✓
	SQL Server on Virtual Machines	✓	✓	✓	✓	✓	✓
	Virtual Machines	✓	✓	✓	✓	✓	✓
	Azure Reserved Virtual Machine Instances	✓	-	✓	✓	✓	✓
	Virtual Machines Scale Sets	✓	✓	✓	✓	✓	✓
Networking	Application Gateway	✓	✓	✓	✓	✓	✓
	Azure DNS[6]	✓	✓	✓	✓	✓	✓
	Content Delivery Network	✓	-	-	✓	✓	✓
	ExpressRoute	✓	✓	✓	✓	✓	✓
	Load Balancer	✓	✓	✓	✓	✓	✓
	Network Watcher[6]	✓	✓	✓	✓	✓	✓
	Traffic Manager	✓	✓	✓	✓	✓	✓
	Virtual Network	✓	✓	✓	✓	✓	✓
	VPN Gateway	✓	✓	✓	✓	✓	✓
Storage	Backup	✓	✓	✓	✓	✓	✓
	Data Lake Store	✓	-	✓	✓	✓	✓
	Import / Export	✓	✓	✓	✓	✓	✓
	Site Recovery	✓	✓	✓	✓	✓	✓
	Storage (Blobs, Disks, Files, Queues, Tables) including Cool and Premium	✓	✓	✓	✓	✓	✓
	StorSimple	✓	✓	✓	✓	✓	✓
Web + Mobile	App Service	✓	✓	✓	✓	✓	✓
	App Service: API Apps	✓	✓	✓	✓	✓	✓
	App Service: Mobile Apps	✓	✓	✓	✓	✓	✓
	App Service: Web Apps	✓	✓	✓	✓	✓	✓

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[5]			
		Azure	Azure Government	Q4 2017	Q1 2018	Q2 2018	Q3 2018
	Azure Search	✓	-	✓	✓	✓	✓
	Media Services	✓	✓	✓	✓	✓	✓
Containers	Azure Container Instances (ACI)	✓	-	-	-	✓	✓
	Azure Container Service (ACS)	✓	-	✓	✓	✓	✓
	Azure Kubernetes Service (AKS)	✓	-	-	✓	✓	✓
	Container Registry	✓	-	✓	✓	✓	✓
Databases	Azure Cosmos DB[6]	✓	✓	✓	✓	✓	✓
	Azure Database for MySQL	✓	-	✓	✓	✓	✓
	Azure Database for PostgreSQL	✓	-	✓	✓	✓	✓
	Azure Database Migration Service	✓	-	-	-	✓	✓
	Redis Cache	✓	✓	✓	✓	✓	✓
	SQL Database	✓	✓	✓	✓	✓	✓
	SQL Data Warehouse	✓	✓	✓	✓	✓	✓
	SQL Server Stretch Database	✓	✓	✓	✓	✓	✓
Analytics	Azure Analysis Services[6]	✓	✓	✓	✓	✓	✓
	Azure Data Factory	✓	-	-	-	-	✓
	Data Lake Analytics	✓	-	✓	✓	✓	✓
	HDInsight	✓	✓	✓	✓	✓	✓
	Stream Analytics	✓	-	✓	✓	✓	✓
AI + Machine Learning	Azure Batch AI	✓	-	-	✓	✓	✓
	Azure Bot Service	✓	-	-	✓	✓	✓
	Bing Speech API	✓	-	-	✓	✓	✓
	Cognitive Services Content Moderator	✓	-	-	-	✓	✓

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[5]			
		Azure	Azure Government	Q4 2017	Q1 2018	Q2 2018	Q3 2018
	Cognitive Services Computer Vision API	✓	-	-	-	✓	✓
	Cognitive Services Face API	✓	-	-	-	-	✓
	Cognitive Services Text Analytics API	✓	-	-	-	✓	✓
	Language Understanding Intelligent Service	✓	-	-	-	-	✓
	Microsoft Genomics	✓	-	-	-	-	✓
	Machine Learning Services (also known as Project Vienna Services)	✓	-	-	✓	✓	✓
	Machine Learning Studio	✓	-	✓	✓	✓	✓
	QnAMaker Service	✓	-	-	-	✓	✓
	Speech to Text (formerly known as Custom Speech Service)	✓	✓	✓	✓	✓	✓
	Translator Speech API[7]	✓	✓	-	✓	✓	✓
	Translator Text API[7]	✓	✓	-	✓	✓	✓
	Video Indexer	✓	-	-	-	-	✓
Internet of Things	Event Grid	✓	-	-	✓	✓	✓
	Event Hubs	✓	✓	✓	✓	✓	✓
	Internet of Things (IoT) Hub[6]	✓	✓	✓	✓	✓	✓
	Notification Hubs	✓	✓	✓	✓	✓	✓
Integration	API Management	✓	-	✓	✓	✓	✓
	Data Catalog	✓	-	✓	✓	✓	✓
	Logic Apps	✓	-	✓	✓	✓	✓
	Service Bus	✓	✓	✓	✓	✓	✓
Security + Identity	Azure Active Directory (Free, Basic)	✓	✓	✓	✓	✓	✓

[7] Examination Period for this service for Azure is from July 1, 2018 to September 30, 2018, while the examination period for Azure Government is from January 1, 2018 to September 30, 2018.

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[5]			
		Azure	Azure Government	Q4 2017	Q1 2018	Q2 2018	Q3 2018
	Azure Active Directory (Premium)	✓	-	✓	✓	✓	✓
	Azure Active Directory B2C	✓	-	✓	✓	✓	✓
	Azure Active Directory Domain Services	✓	-	✓	✓	✓	✓
	Azure Information Protection (including Azure Rights Management)	✓	✓	✓	✓	✓	✓
	Key Vault	✓	✓	✓	✓	✓	✓
	Multi-Factor Authentication (MFA)[6]	✓	✓	✓	✓	✓	✓
	Security Center	✓	-	✓	✓	✓	✓
Developer Tools	Application Insights	✓	-	✓	✓	✓	✓
	Application Insights Profiler	✓	-	-	-	-	✓
	Azure DevTest Labs	✓	-	✓	✓	✓	✓
Management Tools	Automation	✓	✓	✓	✓	✓	✓
	Azure Advisor	✓	-	✓	✓	✓	✓
	Azure Monitor[6]	✓	✓	✓	✓	✓	✓
	Azure Policy	✓	-	-	-	✓	✓
	Azure Resource Manager[8]	✓	✓	✓	✓	✓	✓
	Cloud Shell	✓	-	-	✓	✓	✓
	Log Analytics	✓	✓	✓	✓	✓	✓
	Microsoft Azure Portal[8]	✓	✓	✓	✓	✓	✓
	Scheduler	✓	✓	✓	✓	✓	✓

[8] Services for which AICPA Processing Integrity trust principle was examined: Azure Resource Manager, Microsoft Azure Portal, and RDFE.

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[5]			
		Azure	Azure Government	Q4 2017	Q1 2018	Q2 2018	Q3 2018
Azure Supporting Infrastructure Services[8,9]		✓	✓	✓	✓	✓	✓
Microsoft Online Services							
Microsoft Cloud App Security		✓	-	✓	✓	✓	✓
Microsoft Flow		✓	-	✓	✓	✓	✓
Microsoft Graph		✓	-	✓	✓	✓	✓
Microsoft Intune		✓	-	✓	✓	✓	✓
Microsoft Power BI		✓	✓	✓	✓	✓	✓
Microsoft PowerApps		✓	-	✓	✓	✓	✓
Microsoft Stream		✓	-	✓	✓	✓	✓

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:

[9] Azure Government scope boundary for internal services: AAD Application Proxy, ADRS, AD Gateway, Azure Watson, Pilotfish, DNS (AzDNS, iDNS / RR), dSMS, eSTS, Fabric / Compute Manager, IAM - Data Insights and Reporting Service, IAM - Information Worker UX, IAM - Management Admin UX, IAM - Self Service Credentials Management Service, IAM - Shared Backend Services, Jumpboxes, Kusto, MSODS, OneDDoS, OneDeploy Express v2, PhyNet, PAS, Protection Center, RDFE, RDOS, Resource Providers (Compute, Networking, Storage), Service Fabric - RP Clusters, WANetMon, and Workflow. The coverage period for internal services for both Azure and Azure Government is Q4 2017 through Q3 2018 except for those specified with shorter coverage periods in the *Azure Supporting Infrastructure Services* subsection herein.

Domestic

- Santa Clara, CA (BY1/2/3/4/21[10]/22)
- Phoenix, AZ (PHX20, PHX01[11])
- Des Moines, IA (DM1/2/3, DSM05)
- Chicago, IL (CH1/3, CHI20)
- San Antonio, TX (SN1/2/3/4/5/6)
- Ashburn, VA (BL2/3/5/7)
- Boydton, VA (BN1/3/4/6)
- Dallas, TX (DAL[11])
- Los Angeles, CA (LAX[11])
- Miami, FL (MIA[11])
- Bristow, VA (BLU)
- Reston, VA (BL4/6/30)
- Tukwila, WA (TK5)
- Quincy, WA (CO1/2, MWH01)
- Cheyenne, WY (CYS01/04)
- San Jose, CA (SJC31, SJC[11])
- New York, NY (NYC[11])
- Stirling, VA (BL20)
- Boston, MA (BOS01[11])

International

North America

- Toronto, Canada (YTO20, YTO01[11])
- Quebec City, Canada (YQB20)
- Queretaro, Mexico (MEX30[11])

Australia

- Macquarie Park, Australia (SYD03)
- Melbourne, Australia (MEL01)
- Sydney, Australia (SYD21[12], SYD22[12])
- Canberra, Australia (CBR20[12], CBR21[12])

Europe

- Vienna, Austria (VIE)
- Vantaa, Finland (HEL01)
- Athens, Greece (ATH01[11])
- Amsterdam, Netherlands (AM1/2/3, AMS04/05/06[10]/20)
- Durham, United Kingdom (MME20)
- Chessington, United Kingdom (LON20)
- London, United Kingdom (LON21)
- Cardiff, United Kingdom (CWL20)
- Manchester, United Kingdom (MAN30[11])
- Dublin, Ireland (DB3/4/5, DUB06/07[10]/20[10])
- Paris, France (PAR02[11]/20[10]/21/22)
- Marseille, France (MRS20)
- Copenhagen, Denmark (CPH30[11])
- Milan, Italy (MIL30[11])
- Stockholm, Sweden (STO[11])
- Brussels, Belgium (BRU30[11])
- Frankfurt, Germany (FRA[11])

South America

- Campinas, Brazil (CPQ01/02)
- Fortaleza, Brazil (FOR01)
- Rio de Janeiro, Brazil (RIO01)
- Sao Paulo, Brazil (GRU)
- Santiago, Chile (SCL01)
- Humacao, Puerto Rico (PR1)

Asia

- Hong Kong (HK1/2, HKG20)
- New Delhi, India (DEL01[11])
- Mumbai, India (BOM01)
- Dighi, India (PNQ01)
- Ambattur, India (MAA01)
- Osaka, Japan (OSA01/02/20[10])
- Tokyo, Japan (KAW, TYO01/21/22)
- Cyberjaya, Malaysia (KUL01)
- Singapore (SG1/2/3, SIN20)
- Busan, South Korea (PUS01, PUS20)
- Seoul, South Korea (SEL20)
- Taipei, Taiwan (TPE30[11])
- Manila, Philippines (MNL30[11])

Africa

- Johannesburg, South Africa (JNB02[11])
- Cape Town, South Africa (CPT02[11])

[10] Examination period for this datacenter was from January 1, 2018 to September 30, 2018.

[11] Examination period for the edge sites MEX30, YTO01, PAR02, NYC, DAL, CPH30, MIL30 and STO was from October 1, 2017 to September 30, 2018.

Examination period for the edge sites BRU30, TPE30, LAX, MIA and PHX01 was from April 1, 2018 to September 30, 2018.

Examination period for the edge sites ATH01, BOS01, CPT02, DEL01, FRA, JNB02, MAN30, MNL30 and SJC was from July 1, 2018 to September 30, 2018.

[12] Examination period for this datacenter was from July 1, 2018 to September 30, 2018.

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.

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.

Accountability

All Azure and contingent staff are accountable for understanding and adhering to the guidance contained in the Azure Security Policy, and any applicable supporting procedures. Individuals not employed by Azure, 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 throughout the year 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.

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. **Customer Data** is the data, information, or content that Azure's customers (including their end-users) store or process within Azure through the use of the Azure service. Customer Data comprises all the data-which may include images, text, code or software-provided by the customer or on the customer's behalf.

2. **End-user Identifiable Information (EII)** is information about the end-users of services hosted in Azure that may be visible to Microsoft, e.g., end-user Internet Protocol (IP) addresses.

3. **Access Control Data** is data used to manage access to other types of data or functions within Azure.

4. **Account Data: Payment Information** is information about payment instruments, this type of data is not stored in the Azure platform.

5. **Account Data: Administrator Data** is information about administrators including contact information that is needed to provide the agreed upon service.

6. **Organization Identifiable Information (OII)** is system metadata (configuration, usage, events) when tied to organizations, that own the account or subscription, can be seen as sensitive if used outside of the Azure production environment. This is particularly meaningful to services used by Office 365 and similar SaaS services, so is called out as a separate sub-category for more secure handling.

7. **System Metadata** is configuration, usage and event data, that does not have customer data or any other category of data described above.

Data Ownership

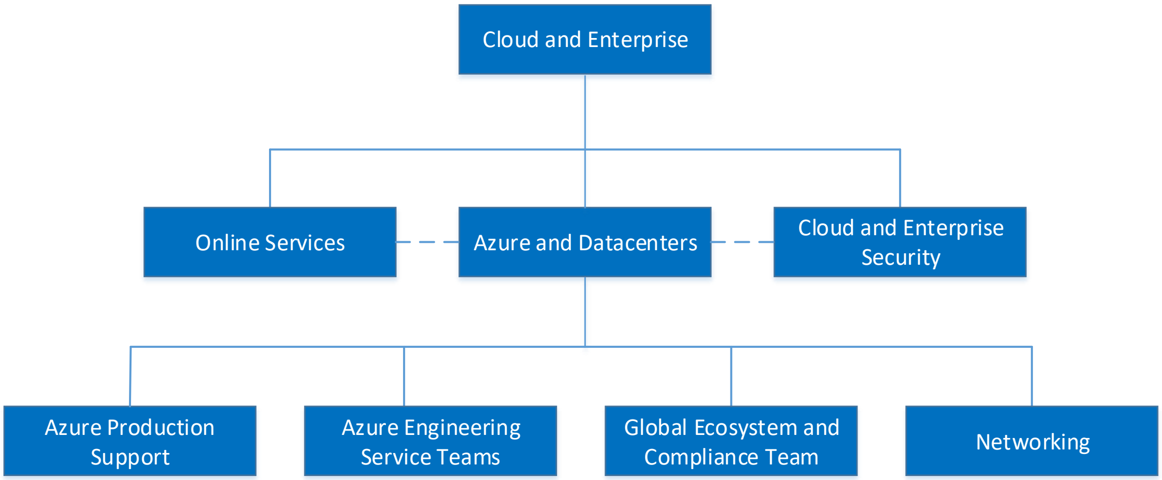
Microsoft does not inspect, approve, or monitor applications that customers deploy to Azure. Moreover, Microsoft does not know what kind of data customers choose to store in Azure. Microsoft does not claim data ownership over the customer information entered into Azure. Azure's Agreement states, "Customers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


Cloud and Enterprise
Online Services
Azure and Datacenters
Cloud and Enterprise Security
Azure Production Support
Azure Engineering Service Teams
Global Ecosystem and Compliance Team
Networking

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 and Enterprise Security

The Cloud and Enterprise Security team works to make Azure a secure and compliant cloud platform by building common security technologies, tools, processes, and best practices. The Cloud and Enterprise 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

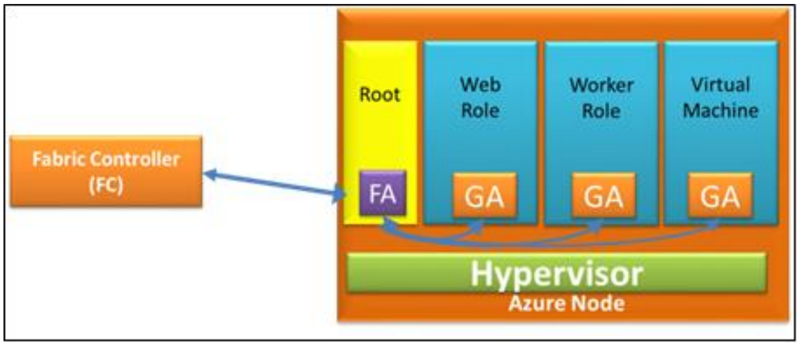
The Networking team is responsible for implementing, monitoring and maintaining the Microsoft network. This team consists of personnel responsible for:

- 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

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

Compute

Azure Migrate: Azure Migrate allows customers discovery and assessment of their on-premise applications and VMs, provides a mapping to Azure VMs and helps migrate them to right-sized Azure VMs. It allows for dependency visualization to view dependencies of a single VM or a group of VMs.

Batch: Batch makes it possible to run large-scale parallel and High-performance Computing (HPC) workloads in Azure. 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 removes the need to manage server infrastructure. It lets customers build, deploy, and manage modern applications with web and worker roles.

Functions: Functions is an event driven, compute-on-demand experience. Customers can leverage Azure Functions to build HTTP endpoints accessible by mobile and IoT devices.

Service Fabric: Service Fabric is a micro-services platform used to build scalable managed applications for the cloud. Service Fabric addresses significant challenges in developing and managing cloud applications by allowing developers and administrators to shift focus from infrastructure maintenance to implementing mission-critical, demanding workloads.

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

Virtual Machines: Virtual Machines, which include Azure Reserved Virtual Machine Instances, lets customers deploy a Windows Server or Linux image in the cloud. Customers can select images from a marketplace or use their own customized images.

Virtual Machine Scale Sets: Virtual Machine Scale Sets 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 and are fully integrated with Azure load balancing and autoscale, as well as support Windows, Linux, custom images, and extensions.

Networking

Application Gateway: Application Gateway is an Azure-managed layer-7 solution providing HTTP load balancing, Secure Sockets Layer (SSL) termination service, and session-based cookie affinity to Internet-facing or internal web applications.

Azure DNS: Azure DNS lets customers host their Domain Name System (DNS) domains alongside their Azure apps and manage DNS records by using their existing Azure subscription.

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.

ExpressRoute: ExpressRoute lets customers create private connections between Azure datacenters and infrastructure that's on customers' premises or in a colocation environment.

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 lets customers route incoming traffic across multiple hosted Azure services running in the same datacenter or in different datacenters across the world.

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 ExpressRoute service.

VPN Gateway: VPN Gateway lets customers establish secure, cross-premises connections between their virtual network within Azure and on-premises IT infrastructure.

Storage

Backup: Backup protects Windows client data and shared files and folders on customer's corporate laptops. Additionally, Backup protects Microsoft SharePoint, Exchange, SQL Server, Hyper-V virtual machines, and other applications in customer's datacenter, integrated with System Center Data Protection Manager (DPM). 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.

Data Lake Store: Data Lake Store 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.

Import / Export: 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.

Site Recovery: Site Recovery contributes to a customer's Business Continuity and Disaster Recovery (BCDR) strategy by orchestrating replication of on-premises physical servers and Virtual Machine servers to Azure or to a secondary datacenter. When a disaster occurs in the customer's primary location, Site Recovery coordinates failover and recovery to the secondary location and ensures that applications / workloads continue to run in the secondary location. Customers can failback their workloads to the primary location when it resumes operations. Site Recovery supports protection and recovery of heterogeneous workloads (including System Center managed / unmanaged Hyper-V workloads, VMware workloads). With 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 tiered application workloads failover together.

Storage: Storage provides distributed persistent storage and five different data storage types: Blob, Disk, File, Queue, and Table. 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. Below are the five different Storage types supported by Azure:

- Blob: Blob contains large amounts of binary data. For example, Blob Storage can be used for an application to store video, or to backup data.

- Disk: Managed and Unmanaged disks are Virtual Hard Disks (VHDs) that are attached to a VM to store application data, or other data that the customer needs to keep.

- File: File Storage offers shared storage for applications using the Server Message Block protocol (SMB). Applications running in Azure VMs, Cloud Services or from on-premises clients can mount a file share in the cloud.

- Queue: Queue provides storage and delivery of messages between one or more applications and roles.

- Table: Table provides fast access to large amounts of structured data that do not require complex SQL queries. For example, Table Storage 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 Blob Storage for cool object 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, low-latency disk support for I/O intensive workloads running on Azure VMs. Customers can attach several Premium Storage disks to a VM. With Premium Storage, applications can have up to 32 TB of storage per VM and achieve 64,000 IOPS (input / output operations per second) per VM with extremely low latencies for read operations. This enables customers to run demanding enterprise workloads including databases, big data and data warehousing on Azure.

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.

Web + Mobile

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

Media Services: 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.

Containers

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

Azure Container Service (ACS): Azure Container Service is a container hosting environment optimized for Azure that provides users the choice of container orchestration platforms such as Mesosphere DC / OS and Docker Swarm.

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.

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, Service Fabric, and others. DevOps teams can manage the configuration of apps isolated from the configuration of the hosting environment. The service 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.

Databases

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 MySQL: Azure Database for MySQL is a MySQL database service built on Microsoft's scalable cloud infrastructure for application developers. 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 PostgreSQL database service built on Microsoft's scalable cloud infrastructure for application developers. 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 database and solve their compatibility, migration and replication issues. The service is designed as a seamless, end-to-end solution for moving on-premises SQL Server databases to the cloud.

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

SQL Database: 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, allowing customers to move and extend to the cloud.

SQL Data Warehouse: SQL Data Warehouse is an elastic data warehouse as a service with enterprise-grade features based on a massively parallel SQL Server processing architecture. It lets customers scale data, either on-premises or in cloud. SQL Data Warehouse lets customers use their existing T-SQL skills 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 Stretch Database: SQL Server Stretch Database dynamically stretches warm and cold transactional data from Microsoft SQL Server to Azure. Unlike typical cold data storage, data is always at hand within SQL Server Stretch Database. Additionally, Stretch Database lets customers provide longer data retention times than typical enterprise storage. Depending on how often customers access the data, they can choose the appropriate level of service, then scale up or down as needed. Using Stretch Database does not require any application changes. Customers can use Stretch Database with new Always Encrypted technology, which helps protect data at rest and in motion.

Analytics

Azure Analysis Services: Azure Analysis Services, based on the proven analytics engine in SQL Server Analysis Services, is an enterprise grade OLAP engine and BI modeling platform, offered as a fully managed platform-as-a-service (PaaS). 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 Factory: Azure Data Factory (ADF) is a service that can orchestrate and operationalize processes to refine enormous stores of raw data into actionable business insights this enables customers to create, schedule, orchestrate, and manage data pipelines at scale.

Data Lake Analytics: Data Lake Analytics is a distributed analytics service built on Apache Yet Another Resource Negotiator (YARN) that dynamically scales so customers can focus on their business goals, not on distributed infrastructure. Instead of deploying, configuring and tuning hardware, customers 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 in Azure VMs, Azure SQL Database, and Azure SQL Data Warehouse.

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 and 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 write 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 Internet of Things (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 or Windows clusters when deploying big data workloads into Azure.

Stream Analytics: Stream Analytics is an event-processing engine that helps customers gain insights from devices, sensors, cloud infrastructure, and existing data properties in real-time. 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. Stream Analytics 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.

AI + Machine Learning

Azure Batch AI: Azure Batch AI is an AI training service build on top of Azure Batch service.

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

Bing Speech API: Bing Speech API is an AI based service that can perform speech recognition from an audio stream, convert text to speech as well as custom grammar-based speech recognition. It is leveraged by multiple teams and products in Microsoft to build speech as an interaction modality, necessary accessibility features and at times also improve productivity.

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 Computer Vision API: Cognitive Services Computer Vision API 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 Face API: Cognitive Services Face API 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 Text Analytics API: Cognitive Services Text Analytics API is a cloud-based service that provides advanced natural language processing over raw text, and includes three main functions: sentiment analysis, key phrase extraction, and language detection.

Language Understanding Intelligent Service: Language Understanding Intelligent Service (LUIS) is a cloud-based API service that enables developers to build their custom languages models (i.e. intent classifier and entity extractor). LUIS applies custom machine-learning intelligence to a user's conversational, natural language text to predict overall meaning, and pull out relevant, detailed information.

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.

Machine Learning Services: Machine Learning Services, also known as Project Vienna Services, are cloud services for data scientists and developers to build intelligent solutions, analyze data, build better models faster, and orchestrate the machine learning development lifecycle with the confidence that data is protected with enterprise-grade security.

Machine Learning Studio: Machine Learning Studio 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.

QnAMaker Service: QnAMaker Service 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.

Speech to Text: Speech to Text, formerly known as Custom Speech Service, is a cloud based service that enables customers to customize and deploy acoustic and language models.

Translator Speech API: Translator Speech API is a cloud-based automatic translation service. The API enables developers to add end-to-end, real-time, speech translations to their applications or services.

Translator Text API: Translator Text API is a cloud-based machine translation service supporting multiple languages that reach more than 95% of world's gross domestic product. Translator can be used to build applications, websites, tools, or any solution requiring multi-language support.

Video Indexer: 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.

Internet of Things

Event Grid: Event Grid is a high scale cloud notification service which enables building event-based micro services. It integrates with any web service for delivering the event notifications.

Event Hubs: Event Hubs enables elastic-scale telemetry and event ingestion with durable buffering and sub-second end-to-end latency for millions of devices and events. Event Hubs is a highly scalable publish-subscribe event ingestor that uses Advanced Message Queuing Protocol (AMQP) and HTTP as its primary interfaces. Event Hubs is a feature of Service Bus that provides a message stream handling capability through a partitioned consumer pattern in which each consumer only reads a specific subset, or partition, of the message stream. This pattern enables horizontal scale for event processing. A partition is an ordered sequence of events that is held in an Event Hub. As newer events arrive, they are added to the end of this sequence. An Event Hub contains multiple partitions. Each partition is independent and contains its own sequence of data.

Internet of Things (IoT) Hub: Internet of Things (IoT) Hub is used to connect, monitor, and control billions of IoT assets running on a broad set of operating systems and protocols. IoT Hub establishes reliable, bi-directional communication with assets, even if they’re intermittently connected, and analyze and act 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. They can also revoke access rights to specific devices to maintain the integrity of their system.

Notification Hubs: Notification Hubs is a massively scalable mobile push notification engine for sending millions of notifications to iOS, Android, Windows, or Kindle devices, working with Apple Push Notification service (APNs), Google Cloud Messaging (GCM), 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.

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.

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.

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 Software as a Service (SaaS) and cloud-based connectors that includes Salesforce, Office 365, Twitter, Dropbox, Google services, and more.

Service Bus: Service Bus is a messaging infrastructure that sits between applications allowing them to exchange messages for improved scale and resiliency. Service Bus allows applications to interact in three ways:

1. Letting applications send and receive messages through a simple queue
2. Using a queue with a publish-and-subscribe mechanism
3. Allowing a connection between applications when queues aren't required

Service Bus provides a hosted, secure, and widely available infrastructure for widespread communication, large-scale event distribution, naming, and service publishing.

Security + Identity

Azure Active Directory: 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. Azure Active Directory comes in 3 editions: Free, Basic, and Premium.

Azure Active Directory B2C: Azure Active Directory B2C extends Azure AD 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 accessible from any device.

Azure Active Directory Domain Services: Azure AD 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 AD Domain Services integrates with the existing Azure AD 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.

Key Vault: Key Vault safeguards keys and other secrets in the cloud by using Hardware Security Modules (HSMs). 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 (MFA): 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.

Security Center: 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.

Developer Tools

Application Insights: Application Insights is an all-in-one telemetry solution that can help customers detect issues, triage impact and solve problems in web apps and services. It provides deep diagnostics and real-time insights while being a seamless part of the Application Lifecycle Management (ALM) processes through Visual Studio, Visual Studio Team Services, and Azure Diagnostics integrations. It supports ASP.NET, J2EE and most of the popular web technologies for web apps on Azure or on customer's own servers.

Application Insights Profiler: Application Insights Profiler is a service that helps users find performance issues in their services by helping them troubleshoot issues in production. Application Insights Profiler helps teams collect performance data in a low-impact way to minimize overhead to the system.

Azure DevTest Labs: Azure DevTest Labs is a service that helps developers and testers quickly create environments in Azure while minimizing waste and controlling cost. Customers can test the latest version of your application by quickly provisioning Windows and Linux environments using reusable templates and artifacts.

Management Tools

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, then provides recommendations that can reduce costs and improve the performance, security, and reliability of applications.

Azure Monitor: Azure Monitor 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.

Azure Policy: Azure Policy is a service used to help customers manage policies in Azure. Azure Policy allows for active control and governance at scale for Azure resources.

Azure Resource Manager: Azure Resource Manager 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 to use for 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 (ARM), 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, customers 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, customers 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, and shell.azure.com.

Log Analytics: Log Analytics lets customers collect, correlate and visualize all their machine data, such as event logs, network logs, performance data, and much 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, separating signals from noise, with powerful log-management capabilities.

Microsoft Azure Portal: Microsoft Azure Portal builds, manages, and monitors all Azure resources 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. Customers manage these Azure applications through the 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 a Storage queue, Service Bus queue, or Service Bus topic on any schedule. Scheduler 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.

Azure Supporting Infrastructure Services

Azure Supporting Infrastructure Services is a collection of internal 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.

Access Control Service: Access Control Service is a feature of Azure Active Directory that provides a process of authenticating and authorizing users to gain access to web applications and services while allowing the features of authentication and authorization to be factored out of the code.

Azure Active Directory Application Proxy[13]: Azure Active Directory Application Proxy provides Single Sign-on (SSO) and secure remote access for web applications hosted on-premises. This can include SharePoint sites, Outlook Web Access, or any other Line of Business (LOB) web applications customers have. These on-premises web applications are integrated with Azure Active Directory (AD), the same identity and control platform that is used by Office 365. End users can then access their on-premises applications the same way they access Office 365 and other SaaS applications integrated with Azure AD. Customers are not required to change the network infrastructure or require VPN to provide this solution for their users.

Azure Active Directory Connect Health: Azure Active Directory Connect Health helps customers monitor and gain insight into their on-premises identity infrastructure and synchronization services by monitoring the health of identity servers and sending notification alerts, providing usage analytics and performance data trends, and reporting on-going activity on the servers.

Azure Active Directory Gateway (ADGateway): ADGateway is an Azure service that acts as a stateless front door / reverse proxy for all requests to other services in Azure AD. ADGateway does not implement any identity / authorization functionality and hence, does not have any customer specific state that is stored. It proxies the requests to the services behind it, routing them appropriately based on the URL and returns the responses from the services to the calling client.

IAM - Management Admin UX (previously named "Azure Active Directory Ibiza UX - Management UX")[13]: 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.

Azure Active Directory Portal Extension for Azure Portal (ADIUX): ADIUX is a stateless user interface service built on top of Ibiza SDK to be used in the Azure Portal to allow Role Based Access Control (RBAC) scenarios, such as enumerating roles, assigning and removing users and groups from roles and vice versa, inviting MSA users into directory in order to assign them to roles etc.

Azure Active Directory Privileged Identity Management: Azure Active Directory 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 AD 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.

[13] Examination Period for this service for Azure Government is from April 1, 2018 to September 30, 2018.

IAM - Data Insights and Reporting Service (previously named "Azure Active Directory Reporting (AXM)")[13]: IAM - Data Insights and Reporting Service provides security and activity reports for Azure Active Directory available to customers.

IAM - Shared Backend Services (previously named "Azure Active Directory User Experience (ADUXP)")[13]: IAM - Shared Backend Services acts as the core data layer that serves the Azure Portal Administrator UX, as well as portions of the Information Worker UX. This data layer connects with various components, including the core directory (MSODS) and OrgID / eSTS in order to provide these experiences.

Azure Device Registration Service (ADRS): ADRS enables customers' employees' devices to be provisioned with an identity. Once the customer sets a policy that allows only compliant devices to access the list of customer defined applications (including Office 365 applications), Azure AD authenticates the device and checks whether the device is compliant before allowing access to the customer defined applications such as Exchange and SharePoint.

Azure Data Movement[14]: Azure Data Movement Storage is a service that enables partner services (Azure Machine Learning, Azure Data Factory) to access/move data across cloud and on-prem.

Azure Front Door (AFD): AFD is a content delivery network service that acts as an Internet gateway for major Microsoft services, such as Bing, Office, MSN, and Skype. It is essentially a network layer between consumers (end users) and the Microsoft services they interface with, for routing user traffic to improve availability, performance, and consistency of user experiences for these services. AFD has multiple gateways distributed around the world through Microsoft datacenters including edge sites, which provides close network proximity to all clients. Once the customer (end user) traffic enters the AFD service, AFD will pick the best Microsoft service endpoint to route the traffic to via intelligent load balancing.

Azure Notification Services: Azure Notification Services enables customers to receive notification for different Azure level outages, maintenance, and audit events.

Azure Monitor - IDC: Azure Monitor - IDC provides mapping from Arm Id of a resource to Internal Id of that resource (and vice versa).

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

Pilotfish: Pilotfish, formerly known as Backend Health Management, 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.

BAPI Connectors[15]: BAPI Connectors provides API access to various SaaS services (like Salesforce, Twitter, Facebook, DropBox, etc.). They enable other Azure based components / services to integrate with these services.

Cloud App Discovery: Cloud App Discovery is a premium feature of Azure Active Directory (AAD) that enables customers to discover cloud applications that are used by the employees in their organization.

Cloud Data Ingestion (CDI): 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

[14] Controls for this service were tested from July 1, 2018 to September 30, 2018.

[15] Controls for this service were tested from January 1, 2018 to September 30, 2018.

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[14]: 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.

Common Data Service (CDS): CDS is a fully extensible data management application platform. CDS provides customers with the ability to bring their data together from across Microsoft Online Services (including Dynamics 365). Customers can then derive insights from this data with Power BI, build or extend applications with PowerApps and the CDS SDK, or automate business processes with Microsoft Flow.

Domain Name System - DNS (AzDNS, iDNS / Recursive Revolvers)

- **AzDNS**: AzDNS is a Domain Name System (DNS) service that hosts critical domains belonging to the Azure platform, as opposed to the customers' domains. For example, each new Storage account or Cloud Service gets a DNS name that is hosted in AzDNS. It is deployed to multiple datacenters globally and uses Anycast to route DNS queries to the closest site.
- **iDNS**: iDNS offers hostname to Dedicated Internet Protocol (DIP) resolution within the customers' Virtual Network (VNet). This allows different VMs / roles in the VNet to refer to each other by a friendly name rather than an IP. This service is Fabric deployed, i.e., 100% VM based, with three tenants and a Storage account in each region for resilience. Each region is independent of other regions in that the records are not stored in other regions and resolvers in other regions are not needed during either provisioning or resolution.
- **Recursive Resolvers (RR)**: Recursive Resolvers provide DNS resolution capabilities to Azure VMs and infrastructure. These servers do not host DNS zones, they perform the task of recursive resolution, which involves the traversal of public DNS records to resolve the name requested by the client. These servers access the Internet but do not provide any services to (and are not accessible from) parties outside of Azure. In each region, there is a cluster of resolvers and each VM / Host is configured with at least two clusters for resilience.

Datacenter Secrets Management Service (dSMS): dSMS is an Azure service that automates secrets generation, their delivery to the consumer services, and periodic rollover at runtime.

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. Fabric Controller and Load Balancer are examples of Azure foundation services; Service Bus and Red Dog Front End (RDFE) are examples of Azure essential services.

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

Evolved Security Token Service (eSTS)[13]: eSTS provides a stateless service that accesses multiple principal and key stores. eSTS absorbs the roles of multiple STSs, so that users see one Azure AD STS. eSTS relies on MSODS to hold information required to complete the authentication. eSTS supports a number of protocols including OAuth 2.0, Open ID Connect, WS-Fed, and Security Assertion Markup Language (SAML) protocol.

Fabric / Compute Manager: Fabric / Compute Manager is a core Azure service that manages Fabric Controllers.

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.

Enterprise Apps (APSSO) (previously named "Identity and Access Management Cloud Password Single Sign On (IAM - Password SSO)"): APSSO provides customers the ability to use a single set of credentials to access both on-premises and online resources. This single set of credentials is managed in the customer's AD and requires Active Directory Federation Services.

IAM - Management UX (previously named "Identity and Access Management Self Service Group Management (IAM - SSGM)"): IAM - Management UX supports group object Create, Read, Update, and Delete (CRUD) operations through Azure AD Graph API. The Graph API provides programmatic access to Azure AD through REST API endpoints. Applications can use the Graph API to perform CRUD operations on directory data and objects.

IAM - Self Service Credentials Management Service (previously named "Identity and Access Management Self Service Password Reset (IAM - SSPR)")[13]: IAM - Self Service Credentials Management Service is a feature of Azure AD that allows Azure AD tenant administrators to register for and subsequently reset their passwords without needing to contact Microsoft support.

Identity and Access Management Sync Fabric (IAM - SF): IAM - SF enables the automatic creation, management and removal of user identities in SaaS applications by connecting to provisioning endpoints provided by application vendors. The SF service ensures that the identities in SaaS applications remain current based on changes in Azure AD. Automated provisioning also extends to user groups.

IAM - Information Worker UX (previously named "Identity and Access Management User Experience (IAMUX)"): IAM - Information Worker UX is a simple Azure service that hosts various pages that information workers interact with to perform daily tasks like managing their profile, changing their passwords, and the like.

Jumpboxes: 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; building out new clusters; managing certificates; and, collecting diagnostics information from production systems. There are multiple Jumpboxes per datacenter. They may be shared inside each region, but typically, a Jumpbox located in one datacenter is used to operate just that datacenter. Jumpboxes are in their own Organizational Unit (OU) and Group Policy Object (GPO). Two-Factor Authentication (2FA) is required for access to all Jumpboxes.

Kusto[13]: Kusto is a near real-time log analytics platform for interactive data exploration that enables Microsoft cloud service teams to understand what is happening across their services and to detect, diagnose, and repair problems. Kusto ingests over 1 trillion events and more than a petabyte of log data per day across hundreds of Microsoft cloud services. It has also been released to customers as Application Insights Analytics.

Managed Service Identity: Managed Service Identity is an Azure service which enables Azure resources to gain secure identities. This, in turn, enables Azure resources to access high value assets using well-established protocols and using the Azure Active Directory as the identity provider. The service manages the issuing of credentials for a given identity, registering them with the directory, rotating them as necessary, and enables provisioning these credentials securely onto the resource host - all without user intervention or exposure to secrets.

MSODS: MSODS is Microsoft Online Directory Services, a feature of Azure Active Directory that also includes Azure Active Directory B2B.

OneDDoS: OneDDoS is a fully automated solution aimed primarily at protecting the underlying infrastructure from Distributed Denial of Service (DDoS) attacks. The OneDDoS mitigation system helps to prevent service interruptions by eliminating harmful volumetric traffic flows. Protecting the infrastructure ensures that attack traffic intended for one customer does not result in collateral damage or diminished network quality of service for other customers. The OneDDoS mitigation system is highly scalable and protects inbound, outbound, and region to region traffic.

OneDeploy Express v2: OneDeploy Express v2 offers a safe and secure method to rollout services to multiple regions across Azure. OneDeploy Express v2 rolls out ARM based templates for IaaS and PaaS services and allows users to 1) manage their rollout orchestration, 2) use system health checks for controlling how the rollouts are orchestrated in a safe manner, and 3) manage their keys and secrets necessary for deployments in Key Vault or dSMS.

OrgID: OrgID is an identity provider for Azure Active Directory. It provides authentication services for identities owned by enterprise customers of Microsoft's Cloud Services, including Azure and Office 365. It is an identity provider for "org-owned" identities that are hosted within cloud as well as a federation provider for identities that a customer prefers to host in their on-premises AD environment. OrgID is accessed via ADGateway. The ADGateway service performs proxy and routing services between OrgID and other services, such as Evolved Security Token Service (eSTS).

PowerApps Authoring: PowerApps Authoring 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 Portal: PowerApps 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 RP for most operations and provides entry points for users to launch into other PowerApps services as necessary.

PowerApps Resource Provider (RP): PowerApps 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 Azure Resource Manager (ARM) resource provider, meaning that incoming requests are authenticated by the ARM front door and proxied through to the RP.

Physical Network (PhyNet): PhyNet is used to provide all datacenter connectivity for Azure. PhyNet is completely transparent to Azure customers who cannot interact directly with any physical network device. The PhyNet service provides APIs to manage network devices in Azure datacenters. PhyNet 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 PhyNet is used to perform certain operations, e.g., enable / disable a port for an unresponsive blade. PhyNet 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.

Policy Administration Service (PAS): PAS is responsible for providing Role Based Access Control (RBAC) capability to an application. Applications can use this capability to create access policy.

Protection Center[13]: Protection Center is a cloud security service that uses state of the art machine learning to analyze terabytes of behavioral and contextual data every day to detect and prevent attempts to attack organizations' Azure AD accounts. This service helps prevent the use of compromised accounts using industry leading machine learning (ML) based real time detection and automated mitigation, helping protect all of the cloud and on-premise applications customers use with Azure AD. Azure AD Identity Protection also notifies the identity admins or security analysts when new compromised users, risky sign-ins, or configuration vulnerabilities are detected in their environment. If Conditional Access policies are enabled, administrators and security analysts can prevent and / or remediate these risks before they are exploited.

RDFE: RDFE is a communication path from the user to the Fabric used to manage Azure services. RDFE represents the publicly exposed classic APIs, which is the front-end to the Azure Portal and the Service Management API (SMAPI). All requests from the user go through the RDFE or the new Azure Resource Manager (ARM).

Red Dog Operating System (RDOS): RDOS provides all Guest and Host Operating Systems for the virtual environment and the services hosted on Azure.

Resource Providers: Resource Providers enable seamless, automated deployment of Compute, Storage, and Networking resources as needed and on demand using the Azure Resource Manager (ARM) templates.

- **Compute Resource Provider (CRP)**: CRP, also referred to as **Compute Platform (CP)**, offers the regional Control Plane for all IaaS-related services. It is always paired with the Network Resource Provider (NRP), Storage Resource Provider (SRP) and the Azure Resource Manager (ARM) as a complete offering.
- **Network Resource Provider (NRP)**: NRP is a regional, highly-available, scalable front-end service for Azure Networking that exposes consistent APIs through the Azure Resource Manager. By being compatible with the Azure Resource Manager, role-based access control, integration with the Azure portal, and template-based deployments are all supported. NRP works with CRP to provide the network support for creating and managing VMs and VM Scale Sets.
- **Storage Resource Provider (SRP)**: SRP enables customers to manage storage accounts and their keys programmatically.

Service Fabric - Resource Provider (RP) Clusters: Service Fabric - RP Clusters provide the runtime and VM hosting capabilities for the core Azure resource providers which include Compute Platform and Network Resource Provider.

WANetMon: WANetMon is a network monitoring tool used primarily by the Operations team to monitor and troubleshoot issues within the Azure network. WANetMon collects different types of data (e.g., Simple Network Management Protocol (SNMP) counters, syslogs, traps) from network devices, processes and corresponding alerts. The Operations team can view this data while troubleshooting networking issues. WANetMon also collects and monitors availability data at datacenter and cluster levels and provides alerts when there is a drop in availability.

Workflow: Workflow provides a highly scalable environment where workflows authored by customers in the Office 365 platform can execute. SharePoint Online allows workflows to be attached to SharePoint sites or lists. This feature enables customers to automate numerous human and document management processes. For every customer who signs up with SharePoint Online, a corresponding tenant is created in the Workflow service (called a scope). Customers who have signed up for Office 365 need not sign up for the Workflow service; setup and configuration of Workflow happens automatically. When the customer authors a SharePoint Workflow and deploys it, SharePoint Online calls into the Workflow service to execute the workflow. Office 365 services including SharePoint Online are not in scope of this SOC report.

Microsoft Cloud App Security

Microsoft Cloud App Security (MCAS): MCAS 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 Flow

Microsoft Flow: Microsoft Flow is a product to help customers set up automated workflows between their favorite apps and services to synchronize files, get notifications, collect data, and more.

Microsoft Graph

Microsoft Graph: Microsoft Graph exposes multiple APIs from Office 365 and other Microsoft cloud services through a single endpoint: https://graph.microsoft.com. Microsoft Graph and Microsoft Graph Webhooks 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 Intune

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

Microsoft Power BI

Power BI: Power BI and Power BI Embedded are 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. And customers can access their data and reports from anywhere with the Power BI Mobile apps, which update automatically with any changes to customers data.

Microsoft PowerApps

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.

Microsoft Stream

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's 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.

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 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. 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 is 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 and Enterprise 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 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 and Enterprise 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 audits 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 access required to perform such audits.

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.

Passwords used to access Azure network devices are restricted to authorized individuals and system processes, such as Fabric, 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 and Enterprise 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+ service 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 seven categories, as described in the Data section above, based on how it is used or may be used within the Service environment.

There are two other types of data which are sometimes referenced in relation to data classification and protection. Azure does not treat these as single categories. Instead, each of these may contain data from one or more data classes described in the Data section above.

1. **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. Administrator PII is "Administrator Data" in the data classification and protected as Medium Business Impact (MBI). End-user PII is protected as Medium Business Impact with Customer Information (MBI+CI).

2. **Support Data (SD):** SD is data or information collected when the customer submits a support request or runs an automated troubleshooter. SD may include information that is from multiple categories above such as System Metadata (e.g., logs), Administrator Data (e.g., administrator IP address) or even Customer Data (e.g., customer's code).

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.

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 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. SSL 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. 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 physical separation between the DEV (development), STAGE (pre-production) and PROD (production) environments. Virtual services run on different clusters in separate network segments. STAGE and PROD environments reside in separate network segments, which are accessed through distinct STAGE and PROD Jumpboxes. Access to STAGE 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 stage 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. 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 and Enterprise 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 and Enterprise 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 and Enterprise 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 and Enterprise 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 and Enterprise 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 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.

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 and Enterprise 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.

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 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. 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.

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

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.

Vulnerability Scanning

Cloud and Enterprise 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 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 that are used for edge production servers are encrypted including the operating system. The drives have Always On encryption and stay encrypted even during OS patching and updates. In addition, all unused IO ports on edge production servers are disabled by OS-level configuration 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.

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

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

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

Access to Customer Virtual Machines

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

Customers can connect to their VMs via the ports and protocols defined by them, create credentials (i.e., username and password) and choose a certificate to encrypt the credentials during initial set-up. 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.

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. 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 Azure 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.

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 three categories for classification: Medium Business Impact (MBI), Medium Business Impact with Customer Information (MBI + CI), and High Business Impact (HBI). 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 quarterly 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.

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 for each in-scope service on the following website: https://azure.microsoft.com/en-us/support/legal/sla/.

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 and events that may impact security, availability 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.

- Legal - Any changes / updates to the Service Agreement, Terms, End User License Agreement (EULA), Acceptable Use Policy (AUP), Privacy Statement or SLAs are posted on the Azure website. The information presented in the Microsoft Trust Center is current as of the “last updated” date at the top of each section, but is subject to change without notice. Customers are encouraged to review the Microsoft Trust Center periodically to be informed of new security, privacy and compliance developments.

- Contact Information - Customers 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 principles and 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	CC5.1, CC5.2, CC5.6, CC7.1, PI1.2, PI1.3, PI1.5
Audit Assurance & Compliance	Security Organization - Information Security Program	CC3.1, CC4.1
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	CC1.3, CC1.4, CC2.1, CC3.1, CC3.2, CC4.1, CC6.1, 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	CC5.2, CC5.5, CC5.8, CC7.1, CC7.2, CC7.4
Data Security & Information Lifecycle Management	Security Organization - Information Security Program, Operator Access, Data Security, Change Management, Software Development, Asset Management, Communications	C1.1, C1.3, C1.7, C1.8, CC2.3, CC3.1, CC5.1, CC5.6, CC5.7, PI1.5
Datacenter Security	Operator Access, Data Security, Physical and Environmental Security, Logical Access, Asset Management	CC3.1, CC5.1, CC5.5, CC5.7
Encryption & Key Management	Operator Access, Data Security, Logical Access	CC5.6, CC5.7
Governance and Risk Management	Security Organization - Information Security Program, Physical and Environmental Security, Baseline Configuration	CC1.2, CC2.3, CC2.5, CC3.1, CC3.2, CC6.2
Human Resources	Security Organization - Information Security Program	CC1.3, CC1.4, CC2.2, CC2.3, CC3.2, CC4.1, CC5.4, CC5.5, CC5.6, CC6.2
Identity & Access Management	Security Organization - Information Security Program, Operator Access, Data Security, Change Management, Software Development, Vulnerability Management, Physical and Environmental Security, Logical	CC3.1, CC5.1, CC5.2, CC5.3, CC7.4

CCM Area	Relevant Description Section	Trust Services Criteria
	Access, Communications, Baseline Configuration	
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, CC6.2, CC4.1, CC5.6, CC6.1
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	C1.4, C1.5, CC2.3, CC2.5, CC4.1, CC5.5, CC6.1, CC6.2
Supply Chain Management, Transparency and Accountability	Security Organization - Information Security Program, Operator Access, Change Management, Software Development, Business Continuity and Resiliency, Communications	C1.4, C1.5, CC2.2, CC2.3, CC5.5
Threat and Vulnerability Management	Software Development, Vulnerability Management, Communications	CC5.6, CC5.8, CC6.1, CC7.1

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.

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 Azure and Microsoft datacenters ("Azure") relating to Azure's in-scope services, 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 Azure's controls on the user entity's internal controls throughout the period October 1, 2017 to September 30, 2018.

This section presents the following information provided by Azure:

- The trust services principles criteria and the CCM criteria specified by the management of Azure
- The controls established and specified by Azure to achieve the criteria for the security, availability, processing integrity and confidentiality principles ("applicable trust services criteria") and the CCM criteria

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 Azure's controls were operating with sufficient effectiveness to achieve the applicable trust services criteria and the CCM criteria. 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 related controls specified by Azure and testing procedures in Section IV of this report, and were not extended to procedures in effect at user organizations.

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 Azure's controls should be evaluated together. If effective user entity controls are not in place, Azure'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 Azure. Our tests were performed on controls as they existed during the period October 1, 2017 to September 30, 2018, and were applied to those controls relating to the applicable trust services criteria and the CCM criteria specified by Azure.

The description of controls is the responsibility of the Azure'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 October 1, 2017 to September 30, 2018.

b. The controls stated in the Description were suitably designed to provide reasonable assurance that the applicable trust services criteria and the CCM criteria would be met if the controls operated effectively throughout the period October 1, 2017 to September 30, 2018.

c. The controls operated effectively to provide reasonable assurance that the applicable trust services criteria and the CCM criteria were met throughout the period October 1, 2017 to September 30, 2018.

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 Azure, our procedures included tests of the following relevant elements of Azure'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 Azure's activities and operations, inspection of Azure's documents and records, and re-performance of the application of Azure'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)

Tests of operating effectiveness

Our tests of the controls were designed to cover a representative number of transactions throughout the period from October 1, 2017 to September 30, 2018. 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 and the CCM criteria to be achieved; (d) the expected efficiency and effectiveness of the tests, and (e) the results of our tests of the control environment.

Testing the accuracy and completeness of information provided by Azure 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 Azure'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
- Azure prepared analysis, schedules, or other evidence manually prepared and utilized by Azure

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 Azure.

Description of testing procedures performed

Deloitte & Touche LLP performed a variety of tests relating to the controls listed in this section throughout the period from October 1, 2017 to September 30, 2018. Our tests of controls were performed on controls as they existed during the period of October 1, 2017 to September 30, 2018 and were applied to those controls relating to in-scope trust principles and the CCM criteria.

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.
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.

Test	Description
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 two parts:

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

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

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

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

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

CC1.0: Common Criteria Related to Organization and Management

Trust Criteria	Azure Activity	Test Result
CC1.1 The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance and monitoring of the system enabling it to meet its commitments and requirements as they relate to security, availability, processing integrity, and confidentiality.	**IS - 1.** A security policy has been established and communicated that defines the information security rules and requirements for the Service environment. **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 to identify and manage compliance with relevant statutory, regulatory and contractual requirements.	No exceptions noted.
CC1.2 Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to security, availability, processing integrity, and confidentiality.	**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. **SOC2 - 20.** Azure performs periodic Information Security Management System (ISMS) reviews and results are reviewed with management. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions. Audit activities are planned and agreed upon in advance by stakeholders and any access required to perform the audits requires approval.	No exceptions noted.
CC1.3 The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security, availability, processing integrity, and confidentiality and provides resources	**IS - 4.** An information security education and awareness program has been established that includes policy training and periodic security updates to Azure personnel. **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.

Trust Criteria	Azure Activity	Test Result
necessary for personnel to fulfill their responsibilities.	being granted access. Additional screening is conducted in accordance with customer specific requirements, for employees with access to applicable data.	
CC1.4 The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to security, availability, processing integrity, and confidentiality.	**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.

CC2.0: Common Criteria Related to Communications

Trust Criteria	Azure Activity	Test Result
CC2.1 Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation.	**IS - 1.** A security policy has been established and communicated that defines the information security rules and requirements for the Service environment. **IS - 4.** An information security education and awareness program has been established that includes policy training and periodic security updates to Azure personnel. **SOC2 - 8.** Azure maintains and distributes an accurate system description to authorized users. **SOC2 - 20.** Azure performs periodic Information Security Management System (ISMS) reviews and results are reviewed with management. This involves monitoring ongoing effectiveness and improvement of the ISMS control	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	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.	
CC2.2 The entity's security, availability, processing integrity, and confidentiality commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.	**IS - 1.** A security policy has been established and communicated that defines the information security rules and requirements for the Service environment. **IS - 4.** An information security education and awareness program has been established that includes policy training and periodic security updates to Azure personnel. **SOC2 - 7.** Azure maintains and communicates the confidentiality and related security obligations for customer data via the Microsoft Trust Center. **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 - 19.** A compliance program is managed with representation from various cross-functional teams to identify and manage compliance with relevant statutory, regulatory and contractual requirements.	No exceptions noted.
CC2.3 The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.	**IS - 1.** A security policy has been established and communicated that defines the information security rules and requirements for the Service environment. **IS - 3.** Management has established defined roles and responsibilities to oversee implementation of the Security Policy across Azure.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	IS - 4. An information security education and awareness program has been established that includes policy training and periodic security updates to Azure personnel. **SOC2 - 7.** Azure maintains and communicates the confidentiality and related security obligations for customer data via the Microsoft Trust Center. **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 - 19.** A compliance program is managed with representation from various cross-functional teams to identify and manage compliance with relevant statutory, regulatory and contractual requirements.	
CC2.4 Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security, availability, processing integrity, and confidentiality of the system, is provided to personnel to carry out their responsibilities.	**IS - 1.** A security policy has been established and communicated that defines the information security rules and requirements for the Service environment. **IS - 4.** An information security education and awareness program has been established that includes policy training and periodic security updates to Azure personnel.	No exceptions noted.
CC2.5 Internal and external users have been provided with information on how to report security, availability, processing integrity, and confidentiality failures, incidents, concerns, and other complaints to appropriate personnel.	**IS - 4.** An information security education and awareness program has been established that includes policy training and periodic security updates to Azure personnel. **IM - 1.** An incident management framework has been established and communicated with defined processes, roles and responsibilities for the detection, escalation and response of incidents. **IM - 3.** The Operations team performs monitoring, including documentation, classification, escalation and coordination of incidents per documented procedures.	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 are 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 submitting complaints. Reported issues are reviewed and addressed per documented incident management procedures.	
CC2.6 System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to security, availability, processing integrity, and confidentiality are communicated to those users in a timely manner.	**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. **IS - 4.** An information security education and awareness program has been established that includes policy training and periodic security updates to Azure personnel.	No exceptions noted.

CC3.0 Common Criteria Related to Risk Management and Design and Implementation of Controls

Trust Criteria	Azure Activity	Test Result
CC3.1 The entity (1) identifies potential threats that could impair system security, availability, processing integrity, and confidentiality commitments and system requirements (including threats arising from the use of vendors and other third parties	**VM - 1.** Azure platform components are configured to log and collect security events. **VM - 2.** Administrator activity in the Azure platform is logged.	**Exception Noted:** **VM - 6:** An exception related to the retention of vulnerability scanning

Trust Criteria	Azure Activity	Test Result
providing goods and services, as well as threats arising from customer personnel and others with access to the system); (2) analyzes the significance of risks associated with the identified threats; (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies); (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control; and (5) reassesses, and revises as necessary, risk assessments and mitigation strategies based on the identified changes.	**VM - 3.** A monitoring system has been implemented to monitor the Azure platform for potential malicious activity and intrusion past service trust boundaries. **VM - 6.** Procedures have been established to monitor the Azure platform components for known security vulnerabilities. **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. **IM - 1.** An incident management framework has been established and communicated with defined processes, roles and responsibilities for the detection, escalation and response of incidents. **BC - 1.** Business Continuity Plans (BCP) have been documented and published 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). Plans are reviewed on an annual basis, at a minimum. **BC - 5.** The Azure Business Continuity Planning Organization (BCPO) conducts a risk assessment to identify and assess continuity risks related to Azure services. **BC - 7.** Datacenter Business Continuity Management (BCM) program has been implemented to respond to Microsoft's Enterprise Business Continuance Initiative. This initiative is intended to ensure that Microsoft is ready to mitigate risks and vulnerabilities and respond to a major disruptive event in a manner that enables the business to continue to operate in a safe, predictable, and reliable way. The BCM charter provides a 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.	records was identified in the quarter previous to the current examination period and, per inquiry of management, remediation for this control was in progress from October 1, 2017 through December 31, 2017. D&T sampled 11 servers subsequent to December 31, 2017, and no additional exceptions were noted.

Trust Criteria	Azure Activity	Test Result
	BC - 8. Datacenter Business Continuity Management Program defines business continuity planning and testing requirements for functions within the datacenters. Datacenters are required to at least annually, 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. 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. **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 should be explicitly defined, documented, and kept up to date for each information system and the organization. **SOC2 - 19.** A compliance program is managed with representation from various cross-functional teams to identify and manage compliance with relevant statutory, regulatory and contractual requirements. **SOC2 - 20.** Azure performs periodic Information Security Management System (ISMS) reviews and results are reviewed with management. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions. 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	

Trust Criteria	Azure Activity	Test Result
	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.	
CC3.2 The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy, reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities, and updates the controls, as necessary.	**BC - 2.** Disaster Recovery procedures have been established for Azure components. The Disaster Recovery procedures are tested on a regular basis. **BC - 6.** Procedures have been established for continuity of critical services provided by third parties. 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 results are reviewed with management. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions. 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.

CC4.0: Common Criteria Related to Monitoring of Controls

Trust Criteria	Azure Activity	Test Result
CC4.1 The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security, availability, processing integrity, and confidentiality, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.	**VM - 3.** A monitoring system has been implemented to monitor the Azure platform for potential malicious activity and intrusion past service trust boundaries. **VM - 4.** Procedures have been established to investigate and respond to the malicious events detected by the Azure monitoring system for timely resolution. **VM - 6.** Procedures have been established to monitor the Azure platform components for known security vulnerabilities. **VM - 9.** Network devices in the scope boundary are configured to log and collect security events, and monitored for compliance with established security standards. **IM - 1.** An incident management framework has been established and communicated with defined processes, roles and responsibilities for the detection, escalation and response of incidents. **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. **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 results are reviewed with management. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions. Audit activities are planned and agreed upon in advance by stakeholders and any access required to perform the audits requires approval.	**Exception Noted:** **VM - 6:** An exception related to the retention of vulnerability scanning records was identified in the quarter previous to the current examination period and, per inquiry of management, remediation for this control was in progress from October 1, 2017 through December 31, 2017. D&T sampled 11 servers subsequent to December 31, 2017, and no additional exceptions were noted.

CC5.0: Common Criteria Related to Logical and Physical Access Controls

Trust Criteria	Azure Activity	Test Result
CC5.1 Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity’s commitments and system requirements as they relate to security, availability, processing integrity, and confidentiality.	**OA - 1.** Administrative access to the Service environment is controlled through defined interfaces that require authentication using appropriate credentials. Privileges (i.e., read, write) are restricted to authorized personnel through designated channels based on job responsibilities. **OA - 2.** Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning employee, contractor, and service provider access to specific applications or information resources. **OA - 3.** Procedures are in place to automatically disable Active Directory (AD) accounts and manually remove any non-AD accounts upon user's leave date. **OA - 4.** User credentials adhere to established corporate standards and group policies for password requirements: - expiration - length - complexity - history 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. **OA - 7.** Procedures have been established for granting temporary access for Azure personnel to customer data and applications upon appropriate approval for customer support or incident handling purposes. **OA - 8.** Authentication over an encrypted Remote Desktop Connection is used for administrator access to the production environment.	**Exception Noted:** **OA - 15:** For 8 of the 30 sampled network devices, evidence related to password rotation was not retained and not available for inspection to corroborate that the passwords were changed on a periodic basis.

Trust Criteria	Azure Activity	Test Result
	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 is performed by FTE managers to validate the appropriateness of access to network devices in the scope boundary. **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 - 18.** Azure network is segregated to separate customer traffic from management traffic. **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. **LA - 3.** Logical segregation is implemented to restrict unauthorized access to other customer tenants. **LA - 9.** Service initializes the resource groups within the management portal based on the customer configured templates. **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 password is allowed	

Trust Criteria	Azure Activity	Test Result
	to be changed. SSPR does not display user identifiable information during 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. **DS - 16.** Each Online Service's customer's data is segregated either logically or physically from other Online Services' customers' data.	
CC5.2 New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security, availability, processing integrity, and confidentiality. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	**OA - 1.** Administrative access to the Service environment is controlled through defined interfaces that require authentication using appropriate credentials. Privileges (i.e., read, write) are restricted to authorized personnel through designated channels based on job responsibilities. **OA - 2.** Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning employee, contractor, and service provider access to specific applications or information resources. **OA - 3.** Procedures are in place to automatically disable Active Directory (AD) accounts and manually remove any non-AD accounts upon user's leave date. **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 have been established for granting temporary access for Azure personnel to customer data and applications upon appropriate approval for customer support or incident handling purposes. **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 is performed by FTE managers to validate the appropriateness of access to network devices in the scope boundary.	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. **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 password is allowed to be changed. SSPR does not display user identifiable information during 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.	
CC5.3 Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security, availability, processing integrity, and confidentiality.	**DS - 16.** Each Online Service's customer's data is segregated either logically or physically from other Online Services' customers' data. **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 For production domains where passwords are not in use, multi-factor authentication is enforced.	**Exception Noted:** **OA - 15:** For 8 of the 30 sampled network devices, evidence related to password rotation was not retained and not available for inspection to corroborate that the passwords were changed on a periodic basis.

Trust Criteria	Azure Activity	Test Result
	OA - 7. Procedures have been established for granting temporary access for Azure personnel to customer data and applications upon appropriate approval for customer support or incident handling purposes. **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 - 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 is implemented to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted service components. **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. **LA - 3.** Logical segregation is implemented to restrict unauthorized access to other customer tenants. **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 password is allowed to be changed. SSPR does not display user identifiable information during password reset. Azure Active Directory password policy requirements are enforced on the new passwords supplied by customer administrators within SSPR	

Trust Criteria	Azure Activity	Test Result
	portal. New passwords supplied by customer administrators are protected during transmission over external networks.	
CC5.4 Access to data, software, functions, and other IT resources is authorized and modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security, availability, processing integrity, and confidentiality.	**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 password is allowed to be changed. SSPR does not display user identifiable information during 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 are in place to automatically disable Active Directory (AD) accounts and manually remove any non-AD accounts upon user's leave date. **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 have been established for granting temporary access for Azure personnel to customer data and applications upon appropriate approval for customer support or incident handling purposes. **OA - 8.** Authentication over an encrypted Remote Desktop Connection is used for administrator access to the production environment.	**Exception Noted:** **OA - 15:** For 8 of the 30 sampled network devices, evidence related to password rotation was not retained and not available for inspection to corroborate that the passwords were changed on a periodic basis.

Trust Criteria	Azure Activity	Test Result
	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 is performed by FTE managers to validate the appropriateness of 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. **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 is implemented to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted service components.	
CC5.5 Physical access to facilities housing the system (for example, datacenters, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity’s commitments and system requirements as they relate to security, availability, processing integrity, and confidentiality.	**PE - 1.** Procedures have been established to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors. **PE - 2.** Security verification and check-in are required for personnel requiring temporary access to the interior datacenter facility including tour groups or visitors. **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.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
CC5.6 Logical access security measures have been implemented to protect against security, availability, processing integrity, and confidentiality threats from sources outside the boundaries of the system to meet the entity’s commitments and system requirements.	**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. **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 SSL or equivalent mechanism(s). **PI - 3.** Microsoft Azure performs input validation to restrict any non-permissible requests to the API. **OA - 13.** Access to network devices in the scope boundary is restricted through a limited number of entry points that require authentication over an encrypted connection. **OA - 14.** Access to network devices in the scope boundary requires two-factor authentication and / or other secure mechanisms. **OA - 16.** Network filtering is implemented to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted service components. **OA - 17.** External traffic to the customer VM(s) is restricted to customer enabled ports and protocols. **VM - 7.** Procedures have been established to configure and monitor network devices in the scope boundary, and resolve issues. **VM - 9.** Network devices in the scope boundary are configured to log and collect security events, and monitored for compliance with established security standards. **ED - 1.** Production servers that reside on edge locations are encrypted at the drive level. **ED - 3.** All unused IO ports on edge servers are disabled through the configuration settings at the OS-level.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
CC5.7 The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to security, availability, processing integrity, and confidentiality.	**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 SSL or equivalent mechanism(s). **DS - 12.** Offsite backup tape destruction guidelines have been established and destruction certificates are retained for expired backup tapes. **OA - 8.** Authentication over an encrypted Remote Desktop Connection is used for administrator access to the production environment. **OA - 13.** Access to network devices in the scope boundary is restricted through a limited number of entry points that require authentication over an encrypted connection. **OA - 14.** Access to network devices in the scope boundary requires two-factor authentication and / or other secure mechanisms.	No exceptions noted.
CC5.8 Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to security, availability, processing integrity, and confidentiality.	**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 has been implemented to monitor the Azure platform for potential malicious activity and intrusion past service trust boundaries. **VM - 4.** Procedures have been established to investigate and respond to the malicious events detected by the Azure monitoring system for timely resolution. **VM - 5.** Procedures have been established to evaluate and implement Microsoft released patches to Service components. **VM - 6.** Procedures have been established to monitor the Azure platform components for known security vulnerabilities. **VM - 7.** Procedures have been established to configure and monitor network devices in the scope boundary, and resolve issues.	**Exception Noted:** **VM - 6:** An exception related to the retention of vulnerability scanning records was identified in the quarter previous to the current examination period and, per inquiry of management, remediation for this control was in progress from October 1, 2017 through December 31, 2017.

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.** Network device patches are evaluated and applied based on defined change management 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 - 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. **IM - 1.** An incident management framework has been established and communicated with defined processes, roles and responsibilities for the detection, escalation and response of incidents. **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. **ED - 2.** Intrusion alerts are sent to the operator when physical access to the edge servers is detected.	D&T sampled 11 servers subsequent to December 31, 2017, and no additional exceptions were noted.

Trust Criteria	Azure Activity	Test Result
	ED - 3. All unused IO ports on edge servers are disabled through the configuration settings at the OS-level.	

CC6.0: Common Criteria Related to System Operations

Trust Criteria	Azure Activity	Test Result
CC6.1 Vulnerabilities of system components to security, availability, processing integrity, and confidentiality breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to security, availability, processing integrity, and confidentiality.	**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. **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 has been implemented to monitor the Azure platform for potential malicious activity and intrusion past service trust boundaries. **VM - 4.** Procedures have been established to investigate and respond to the malicious events detected by the Azure monitoring system for timely resolution. **VM - 5.** Procedures have been established to evaluate and implement Microsoft released patches to Service components. **VM - 6.** Procedures have been established to monitor the Azure platform components for known security vulnerabilities. **VM - 7.** Procedures have been established to configure and monitor network devices in the scope boundary, and resolve issues. **VM - 9.** Network devices in the scope boundary are configured to log and collect security events, and monitored for compliance with established security standards.	**Exception Noted:** **VM - 6:** An exception related to the retention of vulnerability scanning records was identified in the quarter previous to the current examination period and, per inquiry of management, remediation for this control was in progress from October 1, 2017 through December 31, 2017. D&T sampled 11 servers subsequent to December 31, 2017, and no additional exceptions were noted.

Trust Criteria	Azure Activity	Test Result
	VM - 13. Network device patches are evaluated and applied based on defined change management procedures. **IM - 1.** An incident management framework has been established and communicated with defined processes, roles and responsibilities for the detection, escalation and response of incidents. **IM - 3.** The Operations team performs monitoring, including documentation, classification, escalation and coordination of incidents per documented procedures. **DS - 5.** Backups of key Azure service components and secrets are performed regularly and stored in fault tolerant (isolated) facilities. **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. **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 on edge locations are encrypted at the drive level. **ED - 2.** Intrusion alerts are sent to the operator when physical access to the edge servers is detected. **ED - 3.** All unused IO ports on edge servers are disabled through the configuration settings at the OS-level.	

Trust Criteria	Azure Activity	Test Result
CC6.2 Security, availability, processing integrity, and confidentiality incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.	**IM - 1.** An incident management framework has been established and communicated with defined processes, roles and responsibilities for the detection, escalation and response of incidents. **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 are conducted for severe incidents impacting the Azure environment. **IM - 5.** The Cyber Defense Operations Center (CDOC) team provides reports to Cloud and Enterprise management of information security events on a quarterly basis. Problem statements for systemic issues are submitted to ISMF for executive leadership 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 have been established to investigate and respond to the malicious events detected by the Azure monitoring system for timely resolution. **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 are authorized by system owners. System components / assets are tracked in the GDCO ticketing database.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	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 submitting complaints. Reported issues are reviewed and addressed per documented incident management procedures. **ED - 2.** Intrusion alerts are sent to the operator when physical access to the edge servers is detected.	

CC7.0: Common Criteria Related to Change Management

Trust Criteria	Azure Activity	Test Result
CC7.1 The entity's commitments and system requirements, as they relate to security, availability, processing integrity, and confidentiality are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.	**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. **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. **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 by designated owners.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	VM - 13. Network device patches are evaluated and applied based on defined change management procedures. **IS - 1.** A security policy has been established and communicated that defines the information security rules and requirements for the Service environment. **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 there shall be key management policies. **CM - 6.** Procedures have been established to manage changes to network devices in the scope boundary. **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.	
CC7.2 Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to security, availability, processing integrity, and confidentiality.	**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 and 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. **LA - 8.** Private root key belonging to the Azure services are protected from unauthorized access.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	IM - 4. Incident post-mortem activities are conducted for severe incidents impacting the Azure environment. **SOC2 - 1.** Azure assets are classified in accordance with Microsoft Online Services Classification Guidelines. Additionally, Medium Business Impact (MBI) data is classified into a supplemental category, MBI+CI for customer content. Azure has conducted security categorization for its information and information systems and the results are documented, reviewed and approved by the authorizing official. **SOC2 - 2.** Azure services maintain an inventory of key information assets. Procedures are established to review the inventory on a quarterly basis. **SOC2 - 15.** Azure has established baselines for OS deployments. Azure employs mechanisms to re-image production servers with the latest baseline configurations at least once a month or detect and troubleshoot exceptions or deviations from the baseline configuration in the production environment. The Azure OS and component teams review and update configuration settings and baseline configurations at least annually. **SOC2 - 20.** Azure performs periodic Information Security Management System (ISMS) reviews and results are reviewed with management. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions. Audit activities are planned and agreed upon in advance by stakeholders and any access required to perform the audits requires approval. **VM - 5.** Procedures have been established to evaluate and implement Microsoft released patches to Service components. **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.** Network device patches are evaluated and applied based on defined change management procedures.	

Trust Criteria	Azure Activity	Test Result
CC7.3 Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to security, availability, processing integrity, and confidentiality.	**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 have been established to manage changes to network devices in the scope boundary. **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. **CM - 11.** Change management processes include established workflows and procedures to address emergency change requests. **IM - 4.** Incident post-mortem activities are conducted for severe incidents impacting the Azure environment. **SOC2 - 20.** Azure performs periodic Information Security Management System (ISMS) reviews and results are reviewed with management. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions. Audit activities are planned and agreed upon in advance by stakeholders and any access required to perform the audits requires approval. **VM - 13.** Network device patches are evaluated and applied based on defined change management procedures.	No exceptions noted.
CC7.4 Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's security, availability, processing integrity, and	**CM - 1.** Procedures for managing different types of changes to the features are documented and communicated. **CM - 2.** Key stakeholders approve changes prior to release into production based on documented change management procedures.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
confidentiality commitments and system requirements.	**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 an 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 have been established to manage changes to network devices in the scope boundary. **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. **CM - 11.** Change management processes include established workflows and procedures to address emergency change requests. **VM - 13.** Network device patches are evaluated and applied based on defined change management procedures.	

A1.0: Additional Criteria for Availability

Trust Criteria	Azure Activity	Test Result
A1.1 Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help	**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.

Trust Criteria	Azure Activity	Test Result
meet the entity’s availability commitments and system requirements.	**BC - 7.** Datacenter Business Continuity Management (BCM) program has been implemented to respond to Microsoft's Enterprise Business Continuance Initiative. This initiative is intended to ensure that Microsoft is ready to mitigate risks and vulnerabilities and respond to a major disruptive event in a manner that enables the business to continue to operate in a safe, predictable, and reliable way. The BCM charter provides a 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. **BC - 8.** Datacenter Business Continuity Management Program defines business continuity planning and testing requirements for functions within the datacenters. Datacenters are required to at least annually, 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. 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 are enforced on Azure services 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.	

Trust Criteria	Azure Activity	Test Result
	VM - 12. The availability of Azure services is monitored through third-party and internal tools, and the status is communicated through a Service Dashboard.	
A1.2 Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet the entity's availability commitments and system requirements.	**DS - 5.** Backups of key Azure service components and secrets are performed regularly and stored in fault tolerant (isolated) facilities. **DS - 6.** Critical Azure components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services. **DS - 7.** Customer data is automatically replicated within Azure to minimize isolated faults. Customers are able to determine geographical regions of the data processing and storage including data backups. **DS - 8.** Data Protection Services (DPS) backs up data for properties based on a defined schedule and upon request of the properties. Data is retained according to the data type identified by the property. DPS investigates backup errors and skipped files and follows up appropriately. **DS - 9.** Backup restoration procedures are defined and backup data integrity checks are performed through standard restoration activities. **DS - 11.** Offsite backups are tracked and managed to maintain accuracy of the inventory information. **DS - 13.** Production data is encrypted on backup media. **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. **BC - 2.** Disaster Recovery procedures have been established for Azure components. The Disaster Recovery procedures are tested on a regular basis.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	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 - 6.** Procedures have been established for continuity of critical services provided by third parties. Contracts with third parties are periodically monitored and reviewed for inconsistencies or non-conformance. **BC - 7.** Datacenter Business Continuity Management (BCM) program has been implemented to respond to Microsoft's Enterprise Business Continuance Initiative. This initiative is intended to ensure that Microsoft is ready to mitigate risks and vulnerabilities and respond to a major disruptive event in a manner that enables the business to continue to operate in a safe, predictable, and reliable way. The BCM charter provides a 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. **BC - 8.** Datacenter Business Continuity Management Program defines business continuity planning and testing requirements for functions within the datacenters. Datacenters are required to at least annually, 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. 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. **PE - 6.** Datacenter Management team maintains datacenter-managed 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	

Trust Criteria	Azure Activity	Test Result
	conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.	
A1.3 Recovery plan procedures supporting system recovery are tested to help meet the entity's availability commitments and system requirements.	**BC - 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 - 8.** Datacenter Business Continuity Management Program defines business continuity planning and testing requirements for functions within the datacenters. Datacenters are required to at least annually, 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. 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.	No exceptions noted.

C1.0: Additional Criteria for Confidentiality

Trust Criteria	Azure Activity	Test Result
C1.1. Confidential information is protected during the system design, development, testing, implementation, and change processes to meet the entity's confidentiality commitments and system requirements.	**CM - 3.** Responsibilities for requesting, approving and implementing changes to the Azure platform are segregated among designated personnel. **LA - 4.** Customer data that is designated as "confidential" is protected while in storage within Azure services. **SDL - 3.** Responsibilities for submitting and approving production deployments are segregated within the Azure teams.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	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.	
C1.2. Confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition to meet the entity's confidentiality commitments and system requirements.	**OA - 1.** Administrative access to the Service environment is controlled through defined interfaces that require authentication using appropriate credentials. Privileges (i.e., read, write) are restricted to authorized personnel through designated channels based on job responsibilities. **OA - 2.** Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning employee, contractor, and service provider access to specific applications or information resources. **OA - 3.** Procedures are in place to automatically disable Active Directory (AD) accounts and manually remove any non-AD accounts upon user's leave date. **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 - 7.** Procedures have been established for granting temporary access for Azure personnel to customer data and applications upon appropriate approval for customer support or incident handling purposes. **OA - 9.** User groups and Access Control Lists have been established to restrict access to network devices in the scope boundary. **OA - 12.** A quarterly review is performed by FTE managers to validate the appropriateness of access to network devices in the scope boundary. **OA - 13.** Access to network devices in the scope boundary is restricted through a limited number of entry points that require authentication over an encrypted connection. **OA - 14.** Access to network devices in the scope boundary requires two-factor authentication and / or other secure mechanisms. **OA - 16.** Network filtering is implemented to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted service components. **OA - 18.** Azure network is segregated to separate customer traffic from management traffic.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	LA - 4. Customer data that is designated as “confidential” is protected while in storage within Azure services. **LA - 11.** One Time Passwords (OTPs) used for self-service password reset are randomly generated. OTPs expire after a pre-defined time limit. OTPs sent to the customer administrator are required to be validated before password is allowed to be changed. SSPR does not display user identifiable information during 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. **DS - 3.** Internal communication between key Azure components where customer data is transmitted / involved is secured using SSL or equivalent mechanism(s). **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 have been established for the disposal of Hard Drives. **DS - 12.** Offsite backup tape destruction guidelines have been established and destruction certificates are retained for expired backup tapes. **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 - 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. **ED - 1.** Production servers that reside on edge locations are encrypted at the drive level. **ED - 3.** All unused IO ports on edge servers are disabled through the configuration settings at the OS-level.	

Trust Criteria	Azure Activity	Test Result
C1.3. Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorized parties to meet the entity's confidentiality commitments and system requirements.	**DS - 1.** Cryptographic certificates, keys, 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 - 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 there shall be key management policies. **DS - 10.** Hard Disk Drive destruction guidelines have been established for the disposal of Hard Drives. **DS - 13.** Production data is encrypted on backup media. **DS - 16.** Each Online Service's customer's data is segregated either logically or physically from other Online Services' customers' data. **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. **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.	**Exception Noted:** **DS - 1:** Exceptions were identified in quarters previous to the current examination period and, per inquiry of management, remediation for this control was in progress from October 1, 2017 through December 31, 2017. D&T sampled 25 secrets subsequent to December 31, 2017, and ascertained that they were following the rotation cadence for secrets defined in the documented procedures.

Trust Criteria	Azure Activity	Test Result
C1.4 The entity obtains confidentiality commitments that are consistent with the entity's confidentiality system requirements from vendors and other third parties whose products and services are part of the system and have access to confidential information.	**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.
C1.5 Compliance with the entity's confidentiality commitments and system requirements by vendors and other third parties whose products and services are part of the system is assessed on a periodic and as-needed basis, and corrective action is taken, if necessary.	**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. **BC - 6.** Procedures have been established for continuity of critical services provided by third parties. Contracts with third parties are periodically monitored and reviewed for inconsistencies or non-conformance.	No exceptions noted.
C1.6 Changes to the entity's confidentiality commitments and system requirements are communicated to internal and external users, vendors, and other third parties whose products and services are part of the system.	**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.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
C1.7 The entity retains confidential information to meet the entity’s confidentiality commitments and system requirements.	**DS - 10.** Hard Disk Drive destruction guidelines have been established for the disposal of Hard Drives. **DS - 12.** Offsite backup tape destruction guidelines have been established and destruction certificates are retained for expired backup tapes. **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 - 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.
C1.8 The entity disposes of confidential information to meet the entity’s confidentiality commitments and system requirements.	**DS - 10.** Hard Disk Drive destruction guidelines have been established for the disposal of Hard Drives. **DS - 12.** Offsite backup tape destruction guidelines have been established and destruction certificates are retained for expired backup tapes. **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.

PI1.0: Additional Criteria for Processing Integrity

Trust Criteria	Azure Activity	Test Result
PI1.1 Procedures exist to prevent, or detect and correct, processing errors to meet the entity’s processing integrity commitments and system requirements.	**DS - 5.** Backups of key Azure service components and secrets are performed regularly and stored in fault tolerant (isolated) facilities. **DS - 9.** Backup restoration procedures are defined and backup data integrity checks are performed through standard restoration activities.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	DS - 14. Azure services are configured to automatically restore customer services upon detection of hardware and system failures. **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. **PE - 6.** Datacenter Management team maintains datacenter-managed 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. **ED - 1.** Production servers that reside on edge locations are encrypted at the drive level. **ED - 2.** Intrusion alerts are sent to the operator when physical access to the edge servers is detected. **ED - 3.** All unused IO ports on edge servers are disabled through the configuration settings at the OS-level.	
PI1.2 System inputs are measured and recorded completely, accurately, and timely to meet the entity's processing integrity commitments and system requirements.	**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 Data is processed completely, accurately, and timely as authorized to meet the entity's processing integrity commitments and system requirements.	**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 - 4.** Microsoft Azure segregates and appropriately provisions the services based on request from customer through the portal / API.	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.	
PI1.4 Data is stored and maintained completely, accurately, and in a timely manner for its specified life span to meet the entity’s processing integrity commitments and system requirements.	**DS - 5.** Backups of key Azure service components and secrets are performed regularly and stored in fault tolerant (isolated) facilities. **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 have been established for the disposal of Hard Drives. **DS - 12.** Offsite backup tape destruction guidelines have been established and destruction certificates are retained for expired backup tapes. **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.
PI1.5 System output is complete, accurate, distributed, and retained to meet the entity’s processing integrity commitments and system requirements.	**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 an 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 have been established to manage changes to network devices in the scope boundary.	No exceptions noted.

Trust Criteria	Azure Activity	Test Result
	DS - 16. Each Online Service's customer's data is segregated either logically or physically from other Online Services' customers' data. **IM - 3.** The Operations team performs monitoring, including documentation, classification, escalation and coordination of incidents per documented procedures. **PI - 4.** Microsoft Azure segregates and appropriately provisions the services based on request from customer through the portal / API. **LA - 3.** Logical segregation is implemented to restrict unauthorized access to other customer tenants.	
PI1.6 Modification of data, other than routine transaction processing, is authorized and processed to meet with the entity's processing integrity commitments and system requirements.	**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 an 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 have been established to manage changes to network devices in the scope boundary. **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 have been established for granting temporary access for Azure personnel to customer data and applications upon appropriate approval for customer support or incident handling purposes. **OA - 12.** A quarterly review is performed by FTE managers to validate the appropriateness of access to network devices in the scope boundary.	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. **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 - 14.** Azure services are configured to automatically restore customer services upon detection of hardware and system failures. **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 password is allowed to be changed. SSPR does not display user identifiable information during 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.	

Part B: CCM Criteria, Control Activities provided by Microsoft Azure and Microsoft datacenters, 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 there shall be 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 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	**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
or systematic processing errors, corruption of data, or misuse.		
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 there shall be key management policies. **IS - 1.** A security policy has been established and communicated that defines the information security rules and requirements for the Service environment.	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 results are reviewed with management. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions. 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 results are reviewed with management. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
	Audit activities are planned and agreed upon in advance by stakeholders and any access required to perform the audits requires approval.	
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 should be explicitly defined, documented, and kept up to date for each information system and the organization. **SOC2 - 19.** A compliance program is managed with representation from various cross-functional teams 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	**BC - 1.** Business Continuity Plans (BCP) have been documented and published 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). Plans are reviewed on an annual basis, at a minimum. **BC - 2.** Disaster Recovery procedures have been established for Azure components. The Disaster Recovery procedures are tested on a regular basis. **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
• Owned by a named person(s) who is responsible for their review, update, and approval • 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 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.	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 have been established for continuity of critical services provided by third parties. 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	**SOC2- 8.** Azure maintains and distributes an accurate system description to authorized users.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
available to authorized personnel to ensure the following: • 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 - 2.** Disaster Recovery procedures have been established for Azure components. The Disaster Recovery procedures are tested on a regular basis. **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	**PE - 6.** Datacenter Management team maintains datacenter-managed equipment within the facility according to documented policy and maintenance procedures.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
ensuring continuity and availability of operations and support personnel.		
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 - 2.** Disaster Recovery procedures have been established for Azure components. The Disaster Recovery procedures are tested on a regular basis. **BC - 5.** The Azure Business Continuity Planning Organization (BCPO) conducts a risk assessment to identify and assess 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) have been documented and published 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). 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 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 - 5.** The Azure Business Continuity Planning Organization (BCPO) conducts a risk assessment to identify and assess 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) have been documented and published 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). 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 has been established and communicated with defined processes, roles and responsibilities for the detection, escalation and response of incidents. **IS - 1.** A security policy has been established and communicated that defines the information security rules and requirements for the Service environment. **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 an 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 have been established to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors. **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 on edge locations are encrypted at the drive level. **ED - 3.** All unused IO ports on edge servers 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 have been established to manage changes to network devices in the scope boundary.	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 have been established for granting temporary access for Azure personnel to customer data and applications upon appropriate approval for customer support or incident handling purposes.	

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. Additionally, Medium Business Impact (MBI) data is classified into a supplemental category, MBI+CI for customer content. Azure has conducted security categorization for its information and information systems and the results are 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	**SOC2 - 2.** Azure services maintain an inventory of key information assets. Procedures are established to review the inventory on a quarterly basis. **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
agreement (SLA) compliance impact, and to address any other business risks associated 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 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 is implemented to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted service components.	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. Additionally, Medium Business Impact (MBI) data is classified into a supplemental category, MBI+CI for customer content. Azure has conducted security categorization for its information and information systems and the results are documented, reviewed and approved by the authorizing official. **SOC2 - 2.** Azure services maintain an inventory of key information assets. Procedures are established to review the inventory on a quarterly basis.	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	**CM - 4.** Software releases and configuration changes to the Azure platform are tested based on an established criteria prior to production implementation.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.	**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.	
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. Additionally, Medium Business Impact (MBI) data is classified into a supplemental category, MBI+CI for customer content. Azure has conducted security categorization for its information and information systems and the results are documented, reviewed and approved by the authorizing official. **SOC2 - 2.** Azure services maintain an inventory of key information assets. Procedures are established to review the inventory on a quarterly basis.	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 have been established for the disposal of Hard Drives. **DS - 12.** Offsite backup tape destruction guidelines have been established and destruction certificates are retained for expired backup tapes.	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	**SOC2 - 1.** Azure assets are classified in accordance with Microsoft Online Services Classification Guidelines. Additionally, Medium Business Impact (MBI) data is classified into a supplemental category, MBI+CI for customer content.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
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.	Azure has conducted security categorization for its information and information systems and the results are documented, reviewed and approved by the authorizing official. **SOC2 - 2.** Azure services maintain an inventory of key information assets. Procedures are established to review the inventory on a quarterly basis. **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 are 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 have been established to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors. **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.

CCM Criteria	Azure Activity	Test Result
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 are authorized by system owners. System components / assets are tracked in the GDCO ticketing database.	No exceptions noted.
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 have been established for the disposal of Hard Drives. **DS - 12.** Offsite backup tape destruction guidelines have been established and destruction certificates are retained for expired backup tapes.	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 have been established to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors. **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.	No exceptions noted.
DCS-07 Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to	**PE - 1.** Procedures have been established to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
ensure that only authorized personnel are allowed access.	**PE - 2.** Security verification and check-in are required for personnel requiring temporary access to the interior datacenter facility including tour groups or visitors. **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.	
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 have been established to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors. **PE - 2.** Security verification and check-in are required for personnel requiring temporary access to the interior datacenter facility including tour groups or visitors. **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, 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 there shall be key management policies.	**Exception Noted:** **DS - 1:** Exceptions were identified in quarters previous to the current examination period and, per inquiry of management, remediation for this control was in progress from October 1, 2017 through December 31, 2017. D&T sampled 25 secrets subsequent to December 31, 2017, and ascertained that they were following the rotation cadence for secrets defined in the documented procedures.
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)	**DS - 1.** Cryptographic certificates, keys, 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 there shall be key management policies.	**Exception Noted:** **DS - 1:** Exceptions were identified in quarters previous to the current examination period and, per inquiry of management, remediation for this control was in progress from October 1, 2017 through December 31, 2017.

CCM Criteria	Azure Activity	Test Result
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.		D&T sampled 25 secrets subsequent to December 31, 2017, and ascertained that they were following the rotation cadence for secrets defined in the documented procedures.
EKM-03 Policies and procedures shall be established, and supporting business processes and technical measures 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.	**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 SSL or equivalent mechanism(s). **DS - 13.** Production data is encrypted on backup media. **LA - 4.** Customer data that is designated as "confidential" is protected while in storage within Azure services. **ED - 1.** Production servers that resides on edge locations are encrypted at the drive level.	No exceptions noted.
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 there shall be 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 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.	**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.
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 results are reviewed with management. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions. 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.

CCM Criteria	Azure Activity	Test Result
	SOC2 - 26. Microsoft Azure performs an annual risk assessment that covers security, continuity, and operational risks. As part of this process, threats to security are identified and risks from these threats are formally assessed.	
GRM-03 Managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to their area of responsibility.	**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 has been established that includes policy training and periodic security updates to Azure personnel.	No exceptions noted.
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	**IS - 1.** A security policy has been established and communicated that defines the information security rules and requirements for the Service environment. **PE - 1.** Procedures have been established to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors. **SOC2 - 20.** Azure performs periodic Information Security Management System (ISMS) reviews and results are reviewed with management. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions. 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
• Information systems acquisition, development, and maintenance		
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 results are reviewed with management. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions. 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-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 has been established and communicated that defines the information security rules and requirements for the Service environment. **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 has been established that includes policy training and periodic security updates to Azure personnel.	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.

CCM Criteria	Azure Activity	Test Result
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 results are reviewed with management. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions. 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.
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	**SOC2 - 20.** Azure performs periodic Information Security Management System (ISMS) reviews and results are reviewed with management. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
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 results, threat and vulnerability analysis, and regulatory compliance).	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.	
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-	**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.

CCM Criteria	Azure Activity	Test Result
owned assets shall be returned within an established period.	and information system usage. Employees are required to acknowledge agreements to return Microsoft assets upon termination.	
HRS-02 Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.	**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.
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 has been established that includes policy training and periodic security updates to Azure personnel.	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	**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.

CCM Criteria	Azure Activity	Test Result
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).	**IS - 4.** An information security education and awareness program has been established that includes policy training and periodic security updates to Azure personnel.	
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	**IS - 4.** An information security education and awareness program has been established that includes policy training and periodic security updates to Azure personnel. **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.

CCM Criteria	Azure Activity	Test Result
resources (i.e., BYOD) shall be considered and incorporated as appropriate.		
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 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.	**IS - 4.** An information security education and awareness program has been established that includes policy training and periodic security updates to Azure personnel.	No exceptions noted.
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 inappropriate disclosure and tampering of log data.	**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.
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)	**IS - 1.** A security policy has been established and communicated that defines the information security rules and requirements for the Service environment. **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 is implemented to restrict unauthorized access to other customer tenants. **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.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
• 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) • 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	**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.	

CCM Criteria	Azure Activity	Test Result
• 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. **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.	No exceptions noted.
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 has been established and communicated that defines the information security rules and requirements for the Service environment. **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	**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
per defined segregation of duties to address business risks associated with a user-role conflict of interest.	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 have been established for granting temporary access for Azure personnel to customer data and applications upon appropriate approval for customer support or incident handling purposes.	
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 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.
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.

CCM Criteria	Azure Activity	Test Result
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, 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.	**Exception Noted:** **DS - 1:** Exceptions were identified in quarters previous to the current examination period and, per inquiry of management, remediation for this control was in progress from October 1, 2017 through December 31, 2017. D&T sampled 25 secrets subsequent to December 31, 2017, and ascertained that they were following the rotation cadence for secrets defined in the documented procedures.
IAM-09 Provisioning user access (e.g., employees, contractors, customers (tenants), business partners and / or supplier 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	**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 - 10.** Users are granted access to network devices in the scope boundary upon receiving appropriate approvals. **PE - 1.** Procedures have been established to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
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 - 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.
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	**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.

CCM Criteria	Azure Activity	Test Result
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 - 3.** Procedures are in place to automatically disable Active Directory (AD) accounts and manually remove any non-AD accounts upon user's leave date. **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.	
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) • 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	**LA - 2.** Customer credentials used to access Azure services meet the applicable password policy requirements. **OA - 4.** User credentials adhere to established corporate standards and group policies for password requirements: - expiration - length - complexity - history For production domains where passwords are not in use, multi-factor authentication is enforced. **OA - 14.** Access to network devices in the scope boundary requires two-factor authentication and / or other secure mechanisms.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
(e.g., strong / multi-factor, expireable, non-shared authentication secrets)		
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 forensic investigative capabilities in the event of a security breach.	**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.
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	**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.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
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).	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 have been established to investigate and respond to the malicious events detected by the Azure monitoring system for timely resolution. **ED - 2.** Intrusion alerts are sent to the operator when physical access to the edge servers is detected.	
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. **ED - 3.** All unused IO ports on edge servers are disabled through the configuration settings at the OS-level.	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 accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.	**BC - 10.** The network is monitored to ensure availability and address capacity issues in a timely manner. **CCM - 5.** Microsoft Azure 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 results are reviewed with management. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions. 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
	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 have been established to monitor the Azure platform components for known security vulnerabilities. **SOC2 - 15.** Azure has established baselines for OS deployments. Azure employs mechanisms to re-image production servers with the latest baseline configurations at least once a month or detect and troubleshoot exceptions or deviations from the baseline configuration in the production environment. The Azure OS and component teams review and update configuration settings and baseline configurations at least annually.	**Exception Noted:** **VM - 6:** An exception related to the retention of vulnerability scanning records was identified in the quarter previous to the current examination period and, per inquiry of management, remediation for this control was in progress from October 1, 2017 through December 31, 2017. D&T sampled 11 servers subsequent to December 31, 2017, and no additional exceptions were 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 is implemented to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted service components. **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.	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: • Established policies and procedures	**DS - 16.** Each Online Service's customer's data is segregated either logically or physically from other Online Services' customers' data. **LA - 3.** Logical segregation is implemented to restrict unauthorized access to other customer tenants.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
• 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 SSL or equivalent mechanism(s). **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 there shall be 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 SSL or equivalent mechanism(s). **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 is implemented to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted service components. **VM - 2.** Administrator activity in the Azure platform is logged.	No exceptions noted.
IVS-12 Policies and procedures shall be established, and supporting business	**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
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	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 SSL or equivalent mechanism(s). **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.	
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 is implemented to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted service components. **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 has been implemented to monitor the Azure platform for potential malicious activity and intrusion past service trust boundaries. **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.

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)	**CCM - 7.** 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 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.	**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 SSL or equivalent mechanism(s). **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.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
	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.	**CCM - 8.** 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	**IM - 4.** Incident post-mortem activities are conducted for severe incidents impacting the Azure environment. **SOC2 - 18.** Relevant statutory, regulatory, and contractual requirements and the organization’s approach to meet these requirements should be explicitly defined,	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
/ 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.	documented, and kept up to date for each information system and the organization. **SOC2 - 19.** A compliance program is managed with representation from various cross-functional teams to identify and manage compliance with relevant statutory, regulatory and contractual requirements.	
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 has been established and communicated with defined processes, roles and responsibilities for the detection, escalation and response of incidents. **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 are conducted for severe incidents impacting the Azure environment.	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 shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.	**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 security issues and submitting 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.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
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 - 4.** Incident post-mortem activities are conducted for severe incidents impacting the Azure environment.	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 has been established and communicated with defined processes, roles and responsibilities for the detection, escalation and response of incidents. **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.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
	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 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. **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.	
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.
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 by designated owners.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
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 results are reviewed with management. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions. 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 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	**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 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
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 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		

CCM Criteria	Azure Activity	Test Result
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 have been established for continuity of critical services provided by third parties. 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.
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 have been established for continuity of critical services provided by third parties. 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 results are reviewed with management. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions. 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	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
	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.	
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 have been established for continuity of critical services provided by third parties. 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.

TVM: Threat and Vulnerability Management, Anti-Virus / Malicious Software

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 has been implemented to monitor the Azure platform for potential malicious activity and intrusion past service trust boundaries.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
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 have been established to evaluate and implement Microsoft released patches to Service components. **VM - 6.** Procedures have been established to monitor the Azure platform components for known security vulnerabilities. **VM - 13.** Network device patches are evaluated and applied based on defined change management procedures. **CM - 7.** Secure network configurations are applied and reviewed through defined change management procedures. **CM - 10.** Secure configurations for datacenter software are applied through defined change management procedures.	**Exception Noted:** **VM - 6:** An exception related to the retention of vulnerability scanning records was identified in the quarter previous to the current examination period and, per inquiry of management, remediation for this control was in progress from October 1, 2017 through December 31, 2017. D&T sampled 11 servers subsequent to December 31, 2017, and no additional exceptions were noted.
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	**VM - 3.** A monitoring system has been implemented to monitor the Azure platform for potential malicious activity and intrusion past service trust boundaries.	No exceptions noted.

CCM Criteria	Azure Activity	Test Result
organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.		

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

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
IS - 1	A security policy has been established and communicated that defines the information security rules and requirements for the Service environment.	All in-scope Azure services	• Inquired of the management that a documented security policy exists that specifies the documented rules and requirements applicable to the Microsoft Azure environment. • Obtained Microsoft Azure's Information Security Policy and inspected whether 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.	No exceptions noted.
IS - 2	The Security Policy is reviewed and approved annually by appropriate management.	All in-scope Azure services	• 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.	All in-scope Azure services	• 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 that roles and responsibilities for implementation of the security policy requirements were defined and documented.	No exceptions noted.
IS - 4	An information security education and awareness program has been established that includes policy training	All in-scope Azure services	• 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.	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
	and periodic security updates to Azure personnel.		• Inspected training material to ascertain that it incorporated security policy requirements, and was updated as needed.	
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.	All in-scope Azure services	• 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 list of users with privileged access and ascertained that user access to the relevant domains was restricted to defined security user groups and membership.	No exceptions noted.
OA - 2	Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning employee, contractor, and service provider access to specific applications or information resources.	All in-scope Azure services	• Inquired of the management that access requests require approval by the security group owner or asset owner using the account management tool. • 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.	No exceptions noted.
OA - 3	Procedures are in place to automatically disable Active Directory (AD) accounts and	All in-scope Azure services	• Inquired of the Operations team that procedures are established for disabling terminated user	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
	manually remove any non-AD accounts upon user's leave date.		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, HeadTrax (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 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.	
OA - 4	User credentials adhere to established corporate standards and group policies for password requirements: - expiration - length - complexity - history For production domains where passwords are not in use, multi-factor authentication is enforced.	All in-scope Azure services	• Inquired of management to gain an understanding of the implementation of password standards (e.g., length, complexity, age) and acceptable use guidelines for user credentials created on production domains where passwords are in use. • Obtained and inspected group policies enforced on the corporate domain and production domains where passwords are in use, as well as password requirements configured on the non-AD based Azure administration tools, to ascertain that password standards were enforced. • For production domains where passwords are not in use, observed use of multi-factor authentication with a security PIN and certificate.	No exceptions noted.
OA - 5	Access privileges are reviewed quarterly to determine if access rights are	All in-scope Azure services	• Inquired of management to gain an understanding of the process for performing periodic user access reviews for Microsoft Azure.	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
	commensurate to the user's job duties. Access is modified based on the results of the reviews.		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.	
OA - 6	Production domain-level user accounts for domains where passwords are in use are disabled after 90 days of inactivity.	All in-scope Azure services	• Inquired of the Cloud and Enterprise Security team that procedures are established for disabling user accounts inactive for 90 days in the production environment where passwords are in use. • Obtained and inspected the configuration settings for applicable domains where passwords are in use, to ascertain whether accounts are disabled after 90 days of inactivity. • 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 have been established for granting temporary access for Azure personnel to customer data and applications upon appropriate approval for customer support or incident handling purposes.	All in-scope Azure services	• Inquired of the management to understand the procedures in place for granting and revoking temporary access to internal administration services. • 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	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
			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.	All in-scope Azure services	• 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.	PhyNet	• Inquired of the Networking team that user groups and Access Control Lists (ACLs) are established to restrict access to network devices. • Inquired that 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 boundary upon receiving appropriate approvals.	PhyNet	• Inquired of the Networking team regarding the procedures in place to grant access to new users for network devices in the scope boundary. • Observed the approval process to ascertain that access to a security group was granted upon approval from the network security group owner.	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
			• 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.	PhyNet	• Inquired of the Operations team that 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, HeadTrax (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 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 is performed by FTE managers to validate the appropriateness of access to network devices in the scope boundary.	PhyNet	• Inquired of the Networking team that 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	Service Applicability	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.	PhyNet	• Inquired of the Networking team that 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 were established to restrict user access to network devices in the scope boundary, through a limited number of entry points that require authentication over an encrypted connection. • For a select sample of hop-box servers, performed a walkthrough to ascertain that remote access to network devices involved login to a hopbox server using domain credentials and Smart card followed by login to 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 a sample of hopbox 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.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
OA - 14	Access to network devices in the scope boundary requires two-factor authentication and / or other secure mechanisms.	PhyNet	• Inquired of the Networking team that two-factor authentication is enforced while connecting to a network device. • For a sample network device, observed that login 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.	No exceptions noted.
OA - 15	Passwords used to access Azure network devices are restricted to authorized individuals based on job responsibilities and changed on a periodic basis.	PhyNet	• Inquired of the Networking Team to gain an understanding of: – The network equipment where static passwords exist and the type of static accounts (i.e. 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 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:** For 8 of the 30 sampled network devices, evidence related to password rotation was not retained and not available for inspection to corroborate that the passwords were changed on a periodic basis.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
OA - 16	Network filtering is implemented to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted service components.	Microsoft datacenters and PhyNet	• 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.	All in-scope Azure services	• 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.	Microsoft datacenters and PhyNet	• Inquired of the management regarding the procedures and technical controls used for segregating networks within the Azure environment. • Observed and inspected mechanisms used for segregating and restricting network traffic within the Azure environment.	No exceptions noted.
DS - 1	Cryptographic certificates, keys, customer access keys used for communication between Azure services and other internal components	All in-scope Azure services	• 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.	**Exception Noted:** Exceptions were identified in quarters previous to the current examination period and, per inquiry of

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
	are stored securely and are rotated on a periodic basis.		• 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 via 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 evidences (e.g., tickets, logs) indicating that the secrets were rotated based on the pre-determined frequency. • Performed inquiry and ascertained that master key was secured based on controlled procedures.	management, remediation for this control was in progress from October 1, 2017 through December 31, 2017. D&T sampled 25 secrets subsequent to December 31, 2017, and ascertained that they were following the rotation cadence for secrets defined in the documented procedures.
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.	All in-scope Azure services	• 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 Portal to identify and validate authentication sessions.	No exceptions noted.
DS - 3	Internal communication between key Azure components where customer data is transmitted / involved	All in-scope Azure services	• Inquired of the Azure Operations team to understand the use of secure mechanisms such as Secure Socket Layer (SSL) with mutual authentication for communication between	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
	is secured using SSL or equivalent mechanism(s).		internal Azure components that involves customer data. • For a select sample of Azure platform components, inspected configurations and observed the use of secure mechanisms such as SSL for internal communication.	
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 there shall be key management policies.	All in-scope Azure services	• 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 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.	All in-scope Azure services	• Inquired of the management that 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	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
			were replicated, backed up, and stored in separate locations.	
DS - 6	Critical Azure components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services.	All in-scope Azure 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.	All in-scope Azure services	• 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	Microsoft datacenters	• Inquired of the DPS team regarding the process for scheduling of backups of production database based on customer requests. • Inquired that 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 is consistent with the security categorization assigned to it.	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
	files and follows up appropriately.		• For a select sample of backup scheduling requests, 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.	Microsoft datacenters	• Inquired of the DPS team that 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 have been established for the disposal of Hard Drives.	Microsoft datacenters	• 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.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
DS - 11	Offsite backups are tracked and managed to maintain accuracy of the inventory information.	Microsoft datacenters	• Inquired of the DPS team that processes are established for tracking and managing offsite backups to maintain accuracy of the inventory information. • 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.	No exceptions noted.
DS - 12	Offsite backup tape destruction guidelines have been established and destruction certificates are retained for expired backup tapes.	Microsoft datacenters	• Inquired of the DPS team that offsite backup tape destruction guidelines are established and destruction certificates are retained for expired backup tapes. • 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 evidence to ascertain that media destruction evidence (i.e., request containing the list of expired tapes and corresponding destruction certificates) was retained.	No exceptions noted.
DS - 13	Production data is encrypted on backup media.	Microsoft datacenters	• Inquired of the DPS team that production data is encrypted prior to storage on backup media.	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
			• For a select sample of servers obtained and inspected data encryption configurations to ascertain that production data was being 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.	
DS - 14	Azure services are configured to automatically restore customer services upon detection of hardware and system failures.	All in-scope Azure services	• 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.	All in-scope Azure services	• 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 test 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 either logically or physically from other Online Services' customers' data.	All in-scope Azure services	• Performed inquiry with MSODS' service owner to understand how the MSODS environment enforces logical or physical segregation of customer data.	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
			- Re-performed the control using test domains to ascertain that customer (tenant) data was segregated.	
CM - 1	Procedures for managing different types of changes to the Azure platform have been documented and communicated.	All in-scope Azure services except Microsoft datacenters	- 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 changes, including major release, minor release, hotfix, and configuration changes, were defined.	No exceptions noted.
CM - 2	Key stakeholders approve changes prior to release into production based on documented change management procedures.	All in-scope Azure services except Microsoft datacenters	- 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.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
CM - 3	Responsibilities for requesting, approving and implementing changes to the Azure platform are segregated among designated personnel.	All in-scope Azure services except Microsoft datacenters	• Inquired of the management that segregation of duties is implemented for key responsibilities for requesting, approving and implementing changes to the Azure platform. • 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 an established criteria prior to production implementation.	All in-scope Azure services except Microsoft datacenters	• Inquired of the management about the procedures for managing various types of changes to the Microsoft Azure environment, including testing requirements. • Identified and obtained the population of the production deployments made during the examination period from the ticketing system, for the Microsoft Azure platform. • Selected a sample of changes to production and ascertained that documented procedures for testing were followed prior to deployment.	No exceptions noted.
CM - 5	Implemented changes to the Azure platform are reviewed for adherence to established procedures prior to closure. Changes are rolled back to their previous state in case of errors or security concerns.	All in-scope Azure services except Microsoft datacenters	• Inquired of the management on 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.	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
			- 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.	
CM - 6	Procedures have been established to manage changes to network devices in the scope boundary.	OneDDoS, PhyNet	- Inquired of the Networking team on 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.
CM - 7	Secure network configurations are applied and reviewed through defined change management procedures.	OneDDoS, PhyNet	- Inquired of the Networking team that the implementation and review of secure network configuration standards are followed through defined change management procedures. - Inspected Azure Networking change procedures and tested that change management procedures were established for secure network configuration changes. - Obtained and inspected sample of network change requests and ascertained that changes were documented, tested, reviewed and approved based on the change type.	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
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 and are reviewed annually and relevant configuration changes are communicated to impacted teams (e.g., IPAK team).	Microsoft datacenters	• Inquired of the Cloud and Enterprise Security team that 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.	Microsoft datacenters	• Inquired of the Networking team that change requests are classified, documented, and approved by the Operations Management Team. • Inspected procedures and tested that established procedures cover the process for requesting, documenting (including if the changes were assessed for risk and prioritized), classifying, approving, and executing datacenter changes. • Selected a sample of change requests and tested that changes were classified, approved, and executed in accordance with documented procedures.	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
CM - 10	Secure configurations for datacenter software are applied through defined change management procedures.	Microsoft datacenters	• Inquired of the Server Standards Team that server-based images (IPAKs) are documented and tested. Additionally, inquired that release to production is restricted to appropriate personnel. • Obtained 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.	Microsoft datacenters	• Inquired of the Networking team that 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 Secure Development Lifecycle (SDL) methodology.	All in-scope Azure services except Microsoft datacenters, Jumpboxes, RDOS, and SQL Server on Virtual Machines	• Inquired of the management that Microsoft SDL methodology is followed for the development of new features and major changes to Microsoft Azure platform. • 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.	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
SDL - 2	Applicable operational security and internal control requirements are documented and approved for major releases prior to production deployment.	All in-scope Azure services except Microsoft datacenters, Jumpboxes, RDOS, and SQL Server on Virtual Machines	• 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.	All in-scope Azure services except Jumpboxes and Microsoft datacenters	• Inquired of the service teams that 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 in test or development environments.	All in-scope Azure services except Jumpboxes and Microsoft datacenters	• Inquired of the service teams that changes are developed and tested in separate environments prior to production deployment and production data is not replicated in test or development environments. • For a select sample of services, obtained subscription namespaces to ascertain that separate environments exist for development and testing of changes prior to production deployment. • For the sampled services, inquired of service owners and inspected policies, test scripts or	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
			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 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.	All in-scope Azure services except Jumpboxes and Microsoft datacenters	• 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.	All in-scope Azure services except Microsoft datacenters, Jumpboxes and PhyNet	• 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 semi-annual basis, and signed off by designated owners.	All in-scope Azure services except Microsoft datacenters, Jumpboxes, RDOS, and SQL Server on	• Inquired of the management that an SDL review is performed at least semi-annually for each service with a major release and signed off 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	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
		Virtual Machines	methodology, and sign-offs were obtained from designated owners.	
VM - 1	Azure platform components are configured to log and collect security events.	All in-scope Azure services except PhyNet, RDOS, and SQL Server on Virtual Machines	• 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.	No exceptions noted.
VM - 2	Administrator activity in the Azure platform is logged.	All in-scope Azure services except PhyNet, RDOS, and SQL Server on Virtual Machines	• 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 has been implemented to monitor the Azure platform for potential malicious activity and intrusion past service trust boundaries.	All in-scope Azure services except PhyNet, RDOS and SQL Server on Virtual Machines	• Inquired of the management regarding the monitoring capabilities within the Azure environment 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	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
			signatures to corroborate that they were up to date.	
VM - 4	Procedures have been established to investigate and respond to the malicious events detected by the Azure monitoring system for timely resolution.	All in-scope Azure services	• 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 have been established to evaluate and implement Microsoft released patches to Service components.	All in-scope Azure services except Phynet and SQL Server on Virtual Machines	• Inquired of the management regarding the patch management process within the Azure environment. • Inspected patch management SOP and ascertained that procedures were established for evaluating and implementing released patches within the Azure environment. • For a select sample of servers, obtained and inspected logs and patch details to ascertain that a selection of patches were assessed and implemented into the production environment per documented procedures.	No exceptions noted.
VM - 6	Procedures have been established to monitor the Azure platform components for known security vulnerabilities.	All in-scope Azure services except PhyNet and SQL Server on Virtual Machines	• Inquired that processes are in place to monitor the Azure environment for known security vulnerabilities. • For a select sample of Azure platform components, performed a walkthrough with the control owner to ascertain that scan findings were tracked and remediated.	**Exception Noted:** An exception related to the retention of vulnerability scanning records was identified in the quarter previous to the current examination period

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
			• For a select sample of Azure platform components, selected a sample of scanning events and ascertained that they were monitored for security vulnerabilities as per documented procedures.	and, per inquiry of management, remediation for this control was in progress from October 1, 2017 through December 31, 2017. D&T sampled 11 servers subsequent to December 31, 2017, and no additional exceptions were noted.
VM - 7	Procedures have been established to configure and monitor network devices in the scope boundary, and resolve issues.	PhyNet	• Inquired of the Networking team to ascertain that procedures are established for configuring and monitoring network devices in the scope boundary, 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.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
VM - 9	Network devices in the scope boundary are configured to log and collect security events, and monitored for compliance with established security standards.	PhyNet	• 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 selected 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.	All in-scope Azure services except PhyNet, RDOS, and SQL Server on Virtual Machines	• 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. • 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.	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
VM - 13	Network device patches are evaluated and applied based on defined change management procedures.	PhyNet	• Inquired of the management that the change management procedures are followed when applying patches to network devices. • Obtained and inspected documentation and ascertained that procedures were established for evaluating and implementing patches to network devices. • For a select sample of network devices, obtained and inspected vulnerability and patch details to ascertain that a selection of vulnerabilities or patches were assessed and mitigating procedures were implemented, as applicable, based on defined procedures.	No exceptions noted.
IM - 1	An incident management framework has been established and communicated with defined processes, roles and responsibilities for the detection, escalation and response of incidents.	All in-scope Azure services	• Inquired that information security incidents are managed through designated responsibilities and documented procedures. • Obtained 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.	All in-scope Azure services	• Inquired that events, thresholds and metrics are established to detect and facilitate an alert / notification to incident management teams. • Observed the configuration files and ascertained that automated monitoring and notification was configured for predefined events. • For a select sample of platform components, ascertained that automated notifications were received upon the occurrence of an event meeting the configured specifications.	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
IM - 3	The Operations team performs monitoring, including documentation, classification, escalation and coordination of incidents per documented procedures.	All in-scope Azure services	• Inquired about the procedures for 24x7 monitoring and handling of incidents. • Identified the population of incidents (all severities) in the examination period and obtained 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 are conducted for severe incidents impacting the Azure environment.	All in-scope Azure services	• Inquired that 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 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 to Cloud and Enterprise management of information security events on a quarterly basis. Problem statements for systemic issues are submitted	Microsoft datacenters	• Inquired of the Cyber Defense Operations Center (CDOC) team that reports information security events to Cloud and Enterprise Security management on a quarterly basis. • Obtained and inspected the quarterly report and tested that problem statements for systemic issues were submitted to ISMF for executive leadership review.	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
	to ISMF for executive leadership review.		• Obtained meeting invite and meeting minutes (MoM) to ascertain that the report was reviewed by Cloud and Security Management and ISMF.	
IM - 6	The Cyber Defense Operations Center (CDOC) team performs annual tests on the security incident response procedures.	Microsoft datacenters	• Inquired of the Cyber Defense Operations Center (CDOC) team that 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 have been established to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors.	Microsoft datacenters	• Inquired of the Datacenter Management team that access levels are established and that 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 about 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 – Tour groups / visitors were escorted by designated personnel with escort privileges	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
			– 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 are required for personnel requiring temporary access to the interior datacenter facility including tour groups or visitors.	Microsoft datacenters	• 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.	Microsoft datacenters	• Inquired of the Datacenter Management team that physical access to datacenters is reviewed and verified quarterly.	No exceptions noted.

Control ID	Control Activity	Service Applicability	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.	
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.	Microsoft datacenters	• Inquired of the Datacenter Management team that physical access mechanisms are in place to restrict access to authorized individuals. • 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.
PE - 5	The datacenter facility is monitored 24x7 by security personnel.	Microsoft datacenters	• Inquired of the Datacenter Management team that 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	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
			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.	
PE - 6	Datacenter Management team maintains datacenter-managed equipment within the facility according to documented policy and maintenance procedures.	Microsoft datacenters	• Inquired of the Datacenter Management team that 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 equipment.	No exceptions noted.
PE - 7	Environmental controls have been implemented to protect systems inside datacenter facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression	Microsoft datacenters	• Inquired of the Datacenter Management team that environmental controls are implemented to protect systems inside the datacenters. • Performed a walkthrough at a sample of datacenters and observed that the environmental controls including temperature control, HVAC (heating, ventilation and air conditioning), fire	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
	systems, and power management systems.		detection and suppression systems, and power management systems were in place.	
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.	Microsoft datacenters	• Inquired of the physical security management team that 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	Multiple in-scope Azure services[16]	• Inquired of the service teams to understand the mechanisms implemented to allow customers to configure access or traffic restrictions.	No exceptions noted.

[16] Services applicable for LA - 1 control: ADRS, App Service (Web, Mobile, API), Azure Active Directory (Free, Basic), Azure Active Directory Premium, Azure Active Directory Domain Services, Azure DevTest Labs, Azure Monitor, Azure Notification Services, Azure Resource Manager, Azure Search, Cloud Services, Speech to Text, Compute Platform, Event Hubs, HDInsight, IAM - Information Worker UX, Key Vault, Logic Apps, Microsoft Azure Portal, MSODS, Notification Hubs, Power BI, RDFE, Redis Cache, Scheduler, Service Bus, Service Fabric, Service Fabric - RP Clusters, SQL Data Warehouse, SQL Database, SQL Server Stretch Database, Storage (Blobs, Disks, Files, Queues, Tables) including Cool and Premium, Import / Export, Access Control Service, IAM - Shared Backend Services, Internet of Things (IoT) Hub, Azure Cosmos DB, IAM - Management UX, Machine Learning Studio, Microsoft Graph, Multi Factor Authentication, Enterprise Apps (APSSO), Stream Analytics, Automation, Azure Information Protection, Backup, Media Services, Site Recovery, StorSimple, AAD Application Proxy, API Management, Application Insights, Azure Active Directory B2C, Azure Container Service, Azure Kubernetes Service, Data Catalog, Data Lake Analytics, Data Lake Store, Functions, Microsoft Cloud App Security, Microsoft Flow, Microsoft PowerApps, Power BI Embedded, Intune, Container Registry, Azure Database for PostgreSQL, Azure Database for MySQL, Microsoft Stream, Azure Active Directory Ibiza UX - Management UX, Azure Batch AI, Event Grid, Azure Bot Service, Bing Speech API, Translator Speech API, Translator Text API, Content Delivery Network, Cognitive Services Computer Vision API, Cognitive Services Content Moderator, Cognitive Services Text Analytics API, QnAMaker Service, Azure Data Factory, Cognitive Services, Cognitive Services Face API, Language Understanding Intelligent Service, Microsoft Genomics and Video Indexer.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
	restricted based on customer configured authorization settings.		• 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.	
LA - 2	Customer credentials used to access Azure services meet the applicable password policy requirements.	Multiple in-scope Azure services[17]	• Inquired of the service teams regarding controls in place to enforce that new passwords within Azure conform to the applicable password policy requirements. • Re-performed the control for a select sample of services through various scenarios such as: – Providing sample weak passwords – Tampering Hypertext Transfer Protocol (HTTP) request with weak passwords to ascertain that new password(s) that do not meet applicable password policy requirements were not accepted.	No exceptions noted.
LA - 3	Logical segregation is implemented to restrict	Multiple in-scope Azure services[18]	• Inquired of the service teams to understand the segregation controls implemented to restrict unauthorized access to other customer tenants.	No exceptions noted.

[17] Services applicable for LA - 2 control: App Service (Web, Mobile, API), Azure Active Directory (Free, Basic), Azure Active Directory Premium, Azure DevTest Labs, Azure Search, HDInsight, IAM - Information Worker UX, Logic Apps, Microsoft Azure Portal, SQL Database, SQL Server Stretch Database, IAM - Shared Backend Services, IAM - Management UX, Enterprise Apps (APSSO), Backup, API Management, Azure Active Directory B2C, Azure Container Service, Azure Kubernetes Service, Microsoft Flow, IAM - Self Service Credentials Management Service, Intune, Container Registry, Azure Database for PostgreSQL, Azure Database for MySQL, Microsoft Stream, Azure Batch AI, Azure Active Directory Ibiza UX - Management UX and Cognitive Services Content Moderator.

[18] Services applicable for LA - 3 control: ADRS, Azure Active Directory (Free, Basic), Azure Active Directory Connect Health, Azure Active Directory Domain Services, Azure Active Directory Premium, Azure DevTest Labs, Azure Advisor, Azure Monitor, Azure Notification Services, Azure Resource Manager, Azure Search, Cloud App Discovery, Speech to Text, Event Hubs, HDInsight, IAM - Information Worker UX, Key Vault, Microsoft Azure Portal, Notification Hubs, Power BI, Redis Cache, Scheduler, Service Bus, SQL Data Warehouse, SQL Database, SQL Server Stretch Database, Access Control Service, IAM - Shared Backend Services, Internet of Things (IoT) Hub, Azure Cosmos DB, IAM - Management UX, Machine Learning Studio, Multi Factor Authentication,

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
	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.	
LA - 4	Customer data that is designated as “confidential” is protected while in storage within Azure services.	Multiple in-scope Azure services[19]	- 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.
LA - 6	The jobs configured by the customer administrators are executed within thirty (30) minutes of the scheduled job run and are repeated based	Scheduler, Automation	- 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.	No exceptions noted.

Enterprise Apps (APSSO), Stream Analytics, Automation, Backup, Media Services, Site Recovery, StorSimple, MSODS, API Management, Application Insights, Azure Active Directory B2C, Azure Container Service, Azure Kubernetes Service, Data Lake Analytics, Data Lake Store, Functions, Microsoft Cloud App Security, Microsoft Flow, Microsoft PowerApps, Power BI Embedded, IAM - Self Service Credentials Management Service, Intune, Container Registry, Azure Database for PostgreSQL, Azure Database for MySQL, Microsoft Stream, Azure Active Directory Ibiza UX - Management UX, Azure Analysis Services, Managed Service Identity, Cloud Data Ingestion, Bing Speech API, Translator Speech API, Translator Text API, Machine Learning Services, Security Center, Azure Container Instances, Cognitive Services Computer Vision API, Cognitive Services Content Moderator, Cognitive Services Text Analytics API, QnAMaker Service, Azure Data Factory, Cognitive Services, Cognitive Services Face API, Microsoft Genomics and Video Indexer.

[19] Services applicable for LA - 4 control: Azure Active Directory Domain Services, Azure DevTest Labs, Azure Search, App Service (Web, Mobile, API), Logic Apps, Speech to Text, HDInsight, Key Vault, SQL Database, SQL Server Stretch Database, Access Control Service , Internet of Things (IoT) Hub, Azure Cosmos DB, Machine Learning Studio, Automation, Backup, Media Services, Site Recovery, StorSimple, Azure Container Service, Azure Kubernetes Service, Data Lake Analytics, Data Lake Store, OrgID, Container Registry, Azure Database for PostgreSQL, Azure Database for MySQL, Microsoft Stream, Azure Active Directory Ibiza UX - Management UX, Azure Batch AI, Event Grid, Azure Bot Service, Machine Learning Services, Content Delivery Network, Cognitive Services Computer Vision API, Cognitive Services Content Moderator, Cognitive Services Text Analytics API and QnAMaker Service.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
	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.	
LA - 7	Quotas are enforced on Azure services as configured by the service administrators to protect against availability related issues.	Notification Hubs, Scheduler, Service Bus, Application Insights, Azure Search	• 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	Private root key belonging to the Azure services are protected from unauthorized access.	Key Vault, Azure Information Protection	• 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	Service Applicability	Test Procedures	Results of Tests
LA - 9	Service initializes the resource groups within the management portal based on the customer configured templates.	Azure Resource Manager	• 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.	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.	Scheduler, Access Control Service, Stream Analytics	• 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 password is allowed to be changed. SSPR does not display user identifiable information during password reset. Azure Active Directory password	IAM - Self Service Credentials Management Service	• 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 – Restrict transmission of new passwords to secure protocols through various endpoints over external networks	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
	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.		– 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.	
ED - 1	Production servers that reside on edge locations are encrypted at the drive level.	Front Door	• Inquired of the Front Door team to gain an understanding of the encryption mechanism present at the drive level on production servers.	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
			• For a select sample of edge servers, ascertained that BitLocker was running and the TPM model was enabled.	
ED - 2	Intrusion alerts are sent to the operator when physical access to the edge servers is detected.	Front Door	• Inquired of Front Door team to understand the mechanism of detecting and alerting unauthorized physical access to edge servers. • For a select sample of edge 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 edge servers are disabled through the configuration settings at the OS-level.	Front Door	• Inquired of the Front Door team to understand the configuration settings used to disable unused IO ports on edge servers. • Obtained and inspected the configuration files for a select sample of servers and ascertained that IO ports were disabled on edge servers.	No exceptions noted.
BC - 1	Business Continuity Plans (BCP) have been documented and published 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). Plans are reviewed	All in-scope Azure services	• 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. • Obtained and inspected the review and approval of the RTO / RPO and BCP.	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
	on an annual basis, at a minimum.			
BC - 2	Disaster Recovery procedures have been established for Azure components. The Disaster Recovery procedures are tested on a regular basis.	All in-scope Azure services	• Inquired of the Business Continuity group to understand the requirements and process in place for establishing the Disaster Recovery Procedures (DRP). • Obtained and inspected Disaster Recovery procedures (DRP) for a sample of components and ascertained that they were established, reviewed and tested on a regular basis.	No exceptions noted.
BC - 3	Azure has developed a Business Continuity and Disaster Recovery (BC / DR) Standard Operating Procedure and documentation that includes the defined information security and availability requirements.	All in-scope Azure services	• 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 for critical services, per the defined testing schedule for different loss scenario. Each loss scenario is tested at least annually. Issues identified	All in-scope Azure services	• 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 BC / DR tests, obtained and inspected BC / DR testing plan and results documents, including follow-up documentation for any issues identified.	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
	during testing are resolved during the exercises and plans are updated accordingly.			
BC - 5	The Azure Business Continuity Planning Organization (BCPO) conducts a risk assessment to identify and assess continuity risks related to Azure services.	All in-scope Azure services	• Inquired of the Business Continuity group to understand the processes in place for evaluating events. • 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 services based on revenue and operations considerations.	No exceptions noted.
BC - 6	Procedures have been established for continuity of critical services provided by third parties. Contracts with third parties are periodically monitored and reviewed for inconsistencies or non-conformance.	All in-scope Azure services	• 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 has been implemented to respond to	Microsoft datacenters	• Inquired of Business Continuity Management team to understand the requirements established	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
	Microsoft's Enterprise Business Continuance Initiative. This initiative is intended to ensure that Microsoft is ready to mitigate risks and vulnerabilities and respond to a major disruptive event in a manner that enables the business to continue to operate in a safe, predictable, and reliable way. The BCM charter provides a 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.		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.	
BC - 8	Datacenter Business Continuity Management Program defines business continuity planning and testing requirements for functions within the datacenters. Datacenters are required to at least annually, exercise, test and maintain	Microsoft datacenters	• Inquired of the Business Continuity Management team that 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	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
	the Datacenter Business Continuity Plan for the continued operations of critical processes and required resources in the event of a disruption. 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.		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.	
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.	Microsoft datacenters	• Inquired of the Business Continuity Management team that a resiliency assessment specific to the operations of datacenters is conducted and operated by management on a quarterly basis or prior to proposed significant changes. • Selected a sample quarter and requested the MCIO ERM resiliency assessment and ascertained that: – The BCM Team assigned risk ownership. – Development of risk treatment plans to address risks were specific to datacenter operations.	No exceptions noted.
BC - 10	The network is monitored to ensure availability and address capacity issues in a timely manner.	PhyNet	• Performed inquiry to understand the procedures established to monitor capacity for network devices.	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
			• Obtained and inspected the capacity management reports for a sample of weeks and tested that capacity analysis was performed on network devices and that network capacity issues were resolved in a timely manner as per established 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.	Azure Resource Manager, Microsoft Azure Portal, RDFE	• Inquired of the 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.	Azure Resource Manager, Microsoft Azure Portal, RDFE	• 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.	Azure Resource Manager, Microsoft Azure Portal, RDFE	• Inquired of the 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	Service Applicability	Test Procedures	Results of Tests
PI - 4	Microsoft Azure segregates and appropriately provisions the services based on request from customer through the portal / API.	Azure Resource Manager, RDFE	• Inquired of the 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. Additionally, Medium Business Impact (MBI) data is classified into a supplemental category, MBI+CI for customer content. Azure has conducted security categorization for its information and information systems and the results are documented, reviewed and approved by the authorizing official.	All in-scope Azure services except Azure DevTest Labs, BAPI Connectors, and Microsoft Genomics	• Inquired of the management on the procedures regarding the identification and classification of key information or data. • Obtained the current asset classification document and inspected 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 are established to review the inventory on a quarterly basis.	All in-scope Azure services except Azure DevTest Labs, BAPI Connectors, and Microsoft Genomics	• Inquired of the management on the process for maintaining and reviewing the inventory of key information or data. • For a sample of quarters, sampled services and obtained and inspected asset review completion records within the inventory management tool showing quarterly review of key information assets. Additionally, obtained email	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
			communications to ascertain that changes, if any, were made per the review performed.	
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 are authorized by system owners. System components / assets are tracked in the GDCO ticketing database.	All in-scope Azure services	• Inquired of the management to gain an understanding of the process for transporting or removing assets from datacenters. • Obtained the population of transports performed during the examination period, and selected sample transports. • For the select samples, obtained and inspected the associated tickets from the ticketing system to ascertain that proper authorization was obtained for offsite transports.	No exceptions noted.
SOC2 - 6	Azure maintains a Customer Support website that describes the process for customers and other external users to inform about potential security issues and submitting complaints. Reported issues are reviewed and addressed per documented incident management procedures.	All in-scope Azure services	• Inquired of the management regarding the Customer Support Website and the process for addressing reported customer incidents. • Observed Customer Support Website and inspected 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.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
SOC2 - 7	Azure maintains and communicates the confidentiality and related security obligations for customer data via the Microsoft Trust Center.	All in-scope Azure services	• Inquired of the management on 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. • 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.	No exceptions noted.
SOC2 - 8	Azure maintains and distributes an accurate system description to authorized users.	All in-scope Azure services	• Inquired of the management on the procedures for the development, maintenance, and distribution of the system description. • Obtained Microsoft Azure service description and inspected 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	All in-scope Azure services	• Inquired of the management on 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.	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
	customers are updated on the Azure website in a timely manner.		• Observed the customer Service Dashboard and inspected 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 determined that they accurately reflected the security policies and procedures currently in place for the Microsoft Azure environment.	
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.	All in-scope Azure services	• Inquired of the management on the procedures for the identification of security requirements and how customers must meet these requirements prior to gaining access to Microsoft Azure. • Obtained the End User Licensing Agreement (EULA) or Customer Agreements required by customers to sign / agree to prior to gaining access, and inspected whether 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	All in-scope Azure services	• 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	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
	breach or violate Microsoft Security Policy.		– 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.	
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.	All in-scope Azure services	• Inquired with the Human Resources (HR) team that procedures had been established to perform background checks on new or transferred Microsoft personnel before they were granted access to data and assets. • Obtained and inspected procedures document to ascertain that background screening performed included verification of personal and professional history. • Obtained the total population of new hires from "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.	No exceptions noted.
SOC2 - 13	Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees are provided Microsoft's Employee Handbook, which	All in-scope Azure services	• Inquired with the Human Resources (HR) team that 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	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
	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.		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 policies around notification of incidents were documented.	
SOC2 - 14	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified and regularly reviewed.	All in-scope Azure services	• Inquired of the management on 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 included in the confidentiality or non-disclosure agreements. • Identified the population of individuals that were new to the Microsoft Azure environment. • Obtained and inspected the security policy and procedure agreements signed by an employee, contractor, or third party for a sample of new users.	No exceptions noted.
SOC2 - 15	Azure has established baselines for OS deployments. Azure employs mechanisms to re-image production servers with the latest baseline configurations at	All in-scope Azure services except RDOS, and SQL Server on Virtual Machines	• 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.	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
	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.		• 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.	
SOC2 - 18	Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization.	All in-scope Azure services	• 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 Microsoft Azure Compliance and Corporate, External, and Legal Affairs (CELA) teams occur on a regular basis. • Obtained and inspected policy, procedure, and agreement documents to ascertain that they included relevant and current statutory, regulatory, and contractual requirements.	No exceptions noted.
SOC2 - 19	A compliance program is managed with representation from various cross-functional teams to identify and manage compliance with relevant statutory, regulatory and contractual requirements.	All in-scope Azure services	• Inquired of the management on 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 Security, Transparency, and Blueprint.	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
			• Obtained and inspected meeting invites and meeting minutes to ascertain that the meeting between Microsoft Azure Compliance and various cross-functional teams such as CELA, and Azure Security, Transparency, and Blueprint, 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.	
SOC2 - 20	Azure performs periodic Information Security Management System (ISMS) reviews and results are reviewed with management. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions. Audit activities are planned and agreed upon in advance by stakeholders and any access required to perform the audits requires approval.	All in-scope Azure services	• Inquired of the management on the process for performing the Information Security Management System (ISMS) review. • Inquired of the management on 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.
SOC2 - 25	Security risks related to external parties (such as	All in-scope Azure services	• Inquired of the management on the risk assessment process and how risks are identified	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
	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.		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.	
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.	All in-scope Azure services	• 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.
CCM - 1	Microsoft Azure has established policies for mobile computing devices to meet appropriate security practices	All in-scope Azure services	• Inquired of the management that a documented policy exists that specifies the rules and requirements applicable to mobile computing devices.	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
	prior to being connected to the production environment.		- Obtained and inspected Azure's mobile computing policy to ascertain that it included applicable information security requirements.	
CCM - 2	Microsoft Azure has included a clear desk and clear screen policy which users are provided as a part of onboarding.	All in-scope Azure services	- Inquired of the management that a documented clear desk and clear screen policy exists. - Obtained Microsoft Azure's clear desk and clear screen policy and inspected whether it addressed applicable information security requirements. Additionally, ascertained that the policy was communicated to users as a part of the on-boarding process.	No exceptions noted.
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.	All in-scope Azure services except PhyNet, RDOS, and SQL Server on Virtual Machines	- 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.	No exceptions noted.
CCM - 4	Microsoft Azure components are configured to use Coordinated Universal Time (UTC) time and the clocks are	All in-scope Azure services	- 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	No exceptions noted.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
	synchronized with the domain controller server.		Network Time Protocol (NTP)), which synchronizes with UTC, to ascertain that systems, including domain controllers have a common time reference. • Observed and inspected mechanisms used by Azure including configurations to sync time and clocks across the Azure components, including domain controllers, to UTC.	
CCM - 5	Microsoft Azure Capacity Management team projects future capacity requirements based on internal operational reports, revenue forecasts and inputs from internal component teams.	All in-scope Azure services	• 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 the 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	Multiple in-scope Azure services[20]	• Inquired of the management regarding the list of Application Programming Interfaces (APIs) that Azure offers to the customer.	No exceptions noted.

[20] Services applicable for CCM - 6 control: App Service (Web, Mobile, API), API Management, Application Gateway, Application Insights, Automation, Azure Active Directory (Free, Basic), Azure Batch AI, Azure Container Service, Azure Kubernetes Service, Azure DNS, Event Grid, Network Watcher, Azure Advisor, Azure DevTest Labs, Azure Monitor, Azure Resource Manager, Azure Search, Batch, Bing Speech API, Content Delivery Network, Cloud Services, Data Catalog, Data Lake Analytics, Data Lake Store, DNS (AzDNS, iDNS / RR), Event Hubs, ExpressRoute, Functions, HDInsight, Key Vault, Load Balancer, Log Analytics, Logic Apps, Media Services, Azure Bot Service, Microsoft Cloud App Security, Translator Speech API, Translator Text API, Notification Hubs, NRP, Power BI, Machine Learning Services, Redis Cache, Scheduler, Service Bus, Service Fabric, Service Fabric - RP Clusters, Site Recovery, SQL Database, SQL Server Stretch Database, Storage (Blobs, Disks, Files, Queues, Tables) including Cool and Premium, Import / Export, Storage Resource Provider (SRP), Traffic Manager, SQL Server on Virtual Machines, Virtual Machines Scale Set,

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
	ecosystem of tools and libraries on the Azure Portal.		• 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.	
CCM - 7	Customer data is accessible within agreed upon services in data formats compatible with providing those services.	All in-scope Azure services	• Inquired of the management that data provided to the customer upon request is in an industry-standard format. • Obtained and inspected APIs offered by Azure and ascertained that customer data was accessible within agreed upon services in data formats compatible with providing those services.	No exceptions noted.
CCM - 8	Microsoft Azure has published virtualization industry standards supported within its environment.	Fabric / Compute Manager	• Inquired of the Azure Operations team to understand 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 format (e.g., Open Virtualization Format (OVF)) supported interoperability with third-party products such as Oracle Virtual Box, VMware Workstation and XenSource.	No exceptions noted.

Internet of Things (IoT) Hub, Azure Cosmos DB, Machine Learning Studio, Stream Analytics, Container Registry, Azure Database for PostgreSQL, Azure Database for MySQL, Azure Analysis Services, Security Center, Azure Container Instances, Azure Policy, Cognitive Services Computer Vision API, Cognitive Services Content Moderator, Cognitive Services Text Analytics API, QnAMaker Service, Azure Data Factory, Cognitive Services, Cognitive Services Face API and Language Understanding Intelligent Service.

Control ID	Control Activity	Service Applicability	Test Procedures	Results of Tests
CCM - 9	Microsoft Azure has established forensic procedures to support potential legal action after an information security incident.	All in-scope Azure services	• 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.

Section V:
Supplemental Information Provided by Microsoft Azure

Section V: Supplemental Information Provided by Microsoft Azure

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, tables, queues, files and disks), 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: http://www.microsoft.com/en-us/server-cloud/cloud-os/global-datacenters.aspx
- 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
DS - 1	Cryptographic certificates, keys, customer access keys used for communication between Azure services and other internal components are stored securely and are rotated on a periodic basis.	**Exception Noted:** Exceptions were identified in quarters previous to the current examination period and, per inquiry of management, remediation for this control was in progress from October 1, 2017 through December 31, 2017. D&T sampled 25 secrets subsequent to December 31, 2017, and ascertained that they were following the rotation cadence for secrets defined in the documented procedures.	The secrets noted were passwords used to control access to a tool in the deployment infrastructure that is no longer used by SQL Data Warehouse service. The service team has removed the passwords and will remove all decommissioned secrets from the repository to avoid recurrence of the finding.
OA - 15	Passwords used to access Azure network devices are restricted to authorized individuals	**Exception Noted:** For 8 of the 30 sampled network devices, evidence	Management has re-emphasized the importance of retaining documentation which includes the implementation of an automated password rotation

Control ID	Control Activity	Exception Noted	Management Response
	based on job responsibilities and changed on a periodic basis.	related to password rotation was not retained and not available for inspection to corroborate that the passwords were changed on a periodic basis.	solution that includes forced log retention.
VM - 6	Procedures have been established to monitor the Azure platform components for known security vulnerabilities.	**Exception Noted:** An exception related to the retention of vulnerability scanning records was identified in the quarter previous to the current examination period and, per inquiry of management, remediation for this control was in progress from October 1, 2017 through December 31, 2017. D&T sampled 11 servers subsequent to December 31, 2017, and no additional exceptions were noted.	This sample was related to internal datacenter servers for a new environment that follows standard vulnerability scanning process as defined in the Vulnerability Scanning and Patch Management Process. In this situation, the raw scan results for these servers were not retained for audit purposes. As a result, Management has emphasized the need to retain scan results to the applicable teams.

User Entity Responsibilities

The following list includes user entity responsibilities that Azure assumes its user entities have implemented, but are not required to meet the criteria. User organizations 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 role change / employee termination.
- 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 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 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 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 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 ExpressRoute.
- Customers are responsible for appropriate setup and management of Network Address Translation (NAT) to connect to Azure services using ExpressRoute.
- Customers are responsible for ensuring the NAT IP pool advertised to Microsoft is not advertised to the Internet when utilizing the ExpressRoute service.

- Customers are responsible for adhering to peering requirements with other Microsoft Online Services such as Office 365 when utilizing the ExpressRoute service.
- Customers utilizing the ExpressRoute service are responsible for encrypting their data while in transit.
- Customers utilizing the 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 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.