Microsoft Corporation - Microsoft Azure Including Dynamics 365

(Azure Germany)

SOC 3 Report

April 1, 2019 - March 31, 2020

Table of contents

Section I:
Independent Service Auditors’ Report

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

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

Section I: Independent Service Auditors' Report

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

Scope

We have examined Microsoft Corporation ("Microsoft", the "Service Organization") and T-Systems International GmbH ("T-Systems") accompanying assertions that the controls within in-scope services and offerings including Dynamics 365 for the Azure Germany cloud environment ("system") were effective throughout the period April 1, 2019 to March 31, 2020[1], to provide reasonable assurance that Microsoft's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, and confidentiality ("applicable trust services criteria")[2] set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*AICPA, Trust Services Criteria*). T-Systems is an independent subservice organization providing data custodian and operations services to Microsoft for the Azure Germany system ("T-Systems' services"). The description of the boundaries of the system ("Description") includes those elements of the services provided to Microsoft and the controls designed by Microsoft and operated by T-Systems that are necessary for Microsoft to achieve its service commitments and system requirements based on the applicable trust services criteria.

Service Organization's Responsibilities

Microsoft is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Microsoft's service commitments and system requirements were achieved. Microsoft has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Microsoft is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Subservice Organization's Responsibilities

T-Systems has also provided the accompanying assertion titled "T-Systems' Management Assertion" about the effectiveness of controls within the system. When preparing its assertion, T-Systems is responsible for preparing the portion of the Description related to the services provided to Microsoft and the T-Systems assertion, including the completeness, accuracy, and method of presentation of the Description and assertion; providing the services

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

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

covered by the Description; and operating controls designed by Microsoft*,* which enable Microsoft to achieve its service commitments and system requirements*.*

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the Service Organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and Microsoft's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Microsoft's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Microsoft's service commitments and system requirements based on the applicable trust services criteria

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

Inherent Limitations

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

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

Opinion

In our opinion, management's assertion that the controls within Microsoft's and T-Systems' Azure Germany cloud environment system were effective throughout the period April 1, 2019 to March 31, 2020, to provide reasonable assurance that Microsoft's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Deloitte & Touche LLP

April 30, 2020

Section II:
Management Assertions

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

Section II: Management Assertions

Microsoft's Management Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Microsoft Corporation's ("Microsoft") in-scope services and offerings including Dynamics 365 for the Azure Germany system throughout the period April 1, 2019 to March 31, 2020[3], to provide reasonable assurance that Microsoft's service commitments and system requirements relevant to security, availability, processing integrity, and confidentiality were achieved. Our description of the boundaries of the system is presented in Section III and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period April 1, 2019 to March 31, 2020, to provide reasonable assurance that Microsoft's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, and confidentiality ("applicable trust services criteria")[4] set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. Microsoft's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section IV.

T-Systems International GmbH ("T-Systems") is a subservice organization providing data custodian and operations services to Microsoft for Azure Germany. Section III includes an explanation of T-Systems' services. T-Systems and Microsoft have each provided a separate assertion relevant to their respective services and controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period April 1, 2019 to March 31, 2020, to provide reasonable assurance that Microsoft's service commitments and system requirements were achieved based on the applicable trust services criteria.

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

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

T · · Systems ·

T-Systems' Management Assertion

T-Systems International GmbH ("T-Systems") is a service organization providing data custodian and operations services to Microsoft Corporation ("Microsoft") for Azure Germany. The description of the boundaries of the system includes an explanation of T-Systems' services. This assertion covers only "T-Systems' Responsibilities" (as further described and explained in the description of the boundaries of the system with the associated footnotes). T-Systems and Microsoft have each provided a separate assertion relevant to their respective services and controls.

As relevant to the services provided by T-Systems to Microsoft, T-Systems has maintained the operating effectiveness of controls specified by Microsoft Corporation ("Microsoft") within Microsoft's in-scope services and offerings including Dynamics 365 for the Azure Germany system throughout the period April 1, 2019 to March 31, 2020[5], to provide reasonable assurance that Microsoft's service commitments and system requirements relevant to security, availability, processing integrity, and confidentiality were achieved. Our portion of the description of the boundaries of the system is presented in Section III and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls operated by T-Systems within the system throughout the period April 1, 2019 to March 31, 2020, to provide reasonable assurance that Microsoft's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, and confidentiality ("applicable trust services criteria")[6] set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. Microsoft's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section IV.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

As relevant to the services provided by T-Systems to Microsoft, we assert that the controls within the system were effective throughout the period April 1, 2019 to March 31, 2020, to provide reasonable assurance that Microsoft's service commitments and system requirements were achieved based on the applicable trust services criteria.

T-Systems International, GmbH

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

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

Section III:
Description of the Boundaries of the Azure Germany System

Section III: Description of the Boundaries of the Azure Germany System

Overview of Operations

Business Description

Microsoft Azure Germany ("Azure") is a cloud computing platform for building, deploying and managing applications through Microsoft-supported and third-party managed domestic 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. Azure supports many customers, partners, and government organizations that span across a broad range of products and services, geographies and industries. Azure is designed to meet their security, confidentiality, and compliance requirements.

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

The German datacenters support Azure, Dynamics 365, and Microsoft Online Services ("Online Services"). Online Services such as Graph, Power BI, and others are Software as a Service (SaaS) services that leverage the underlying Azure platform and datacenter infrastructure. See section titled 'Azure Germany Report Scope Boundary' for the Microsoft Azure services and offerings and Online Services that are in scope for this report.

T-Systems International GmbH ("T-Systems") is a German subsidiary of Deutsche Telekom headquartered in Germany. T-Systems is Azure's designated German Data Trustee that controls access to the Azure systems and infrastructure that hold customer data. Microsoft cannot access customer data without approval from and supervision by T-Systems. Azure Engineering Service teams are required to engage and coordinate with T-Systems to support the Azure Germany environment.

"Azure", when referenced in this report, comprises of "Azure Germany", "Dynamics 365", "Online Services", and the supporting datacenters listed in this report.

Azure Germany Report Scope Boundary

Azure Germany is designed to meet strict European Union data protection requirements by having all customer data and related systems reside in Germany with access controlled by T-Systems. The following Azure Germany services and offerings are in scope for this report:

Product Category	Offering / Service	Examination Period Scope[7]			
		Q4 FY19	Q1 FY20	Q2 FY20	Q3 FY20
	Datacenters				
Datacenter and Operations Service		✓	✓	✓	✓
	Azure				
Compute	App Service	✓	✓	✓	✓
	Azure Service Fabric	✓	✓	✓	✓
	Batch	✓	✓	✓	✓
	Cloud Services[8]	✓	✓	✓	✓
	Virtual Machines	✓	✓	✓	✓
	Virtual Machine Scale Sets	✓	✓	✓	✓
Networking	Application Gateway	✓	✓	✓	✓
	Azure DNS	✓	✓	✓	✓
	Azure ExpressRoute	✓	✓	✓	✓
	Load Balancer	✓	✓	✓	✓
	Network Watcher	✓	✓	✓	✓
	Traffic Manager	✓	✓	✓	✓
	Virtual Network	✓	✓	✓	✓
	VPN Gateway	✓	✓	✓	✓
Storage	Azure Backup	✓	✓	✓	✓
	Azure Site Recovery	✓	✓	✓	✓
	Azure Storage (Blobs, Disks, Files, Queues, Tables) including Cool and Premium	✓	✓	✓	✓

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

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

Product Category	Offering / Service	Examination Period Scope[7]			
		Q4 FY19	Q1 FY20	Q2 FY20	Q3 FY20
Databases	Azure Cache for Redis	✓	✓	✓	✓
	Azure Cosmos DB	✓	✓	✓	✓
	Azure SQL Database	✓	✓	✓	✓
	Azure Synapse Analytics	✓	✓	✓	✓
	SQL Server on Virtual Machines	✓	✓	✓	✓
Analytics	Azure Analysis Services	✓	✓	✓	✓
	Azure Data Explorer	✓	✓	✓	✓
	Azure Stream Analytics	✓	✓	✓	✓
	HDInsight	✓	✓	✓	✓
	Power BI Embedded	✓	✓	✓	✓
AI + Machine Learning	Machine Learning Studio (Classic)	✓	✓	✓	✓
Internet of Things	Azure IoT Hub	✓	✓	✓	✓
	Event Hubs	✓	✓	✓	✓
	Notification Hubs	✓	✓	✓	✓
Integration	Service Bus	✓	✓	✓	✓
Identity	Azure Active Directory	✓	✓	✓	✓
Management and Governance	Azure Resource Manager (ARM)[8]	✓	✓	✓	✓
	Microsoft Azure Portal[8]	✓	✓	✓	✓
	Scheduler	✓	✓	✓	✓
Security	Key Vault	✓	✓	✓	✓
	Multi-Factor Authentication	✓	✓	✓	✓
Media	Azure Media Services	✓	✓	✓	✓
Internal Supporting Services		✓	✓	✓	✓

Offering	Examination Period Scope[7]			
	Q4 FY19	Q1 FY20	Q2 FY20	Q3 FY20
Microsoft Online Services				
Microsoft Graph	✓	✓	✓	✓
Power BI	✓	✓	✓	✓

Offering	Examination Period Scope[7]			
	Q4 FY19	Q1 FY20	Q2 FY20	Q3 FY20
Dynamics 365				
Dynamics 365 Customer Engagement	✓	✓	✓	✓
Dynamics 365 Portals	✓	✓	✓	✓
Dynamics 365 Sales	✓	✓	✓	✓

Locations Covered by this Report

Azure production infrastructure is located in nationally 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 local 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:

Germany	
Biere, Germany (LEJ20)	Frankfurt, Germany (FRA20)

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.

Data

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

1. **Access Control Data** is data used to manage access to administrative roles or sensitive functions.

2. **Customer Content** is the data, information and code that Microsoft internal employees, and non-Microsoft personnel (if present) provide to, transfer in, store in or process in a Microsoft Online Service or product.

3. **End User Identifiable Information (EUII)** is data that directly identifies or could be used to identify the authenticated user of a Microsoft service. EUII does not extend to other personal information found in Customer Content.

4. **Support Data** is data provided to Microsoft and generated by Microsoft as part of support activities.

5. **Account Data** is information about payment instruments. This type of data is not stored in the Azure platform.

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

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

8. **Organization Identifiable Information (OII)** is data that can be used to identify a particular tenant / Azure subscription / deployment / organization (generally configuration or usage data) and is not linkable to a user.

9. **System Metadata** is data generated in the course of running the service, not linkable to a user or tenant. It does not contain Access Control Data, Customer Content, EUII, Support Data, Account Data, Public Personal Data, EUPI, or OII.

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

Data Ownership

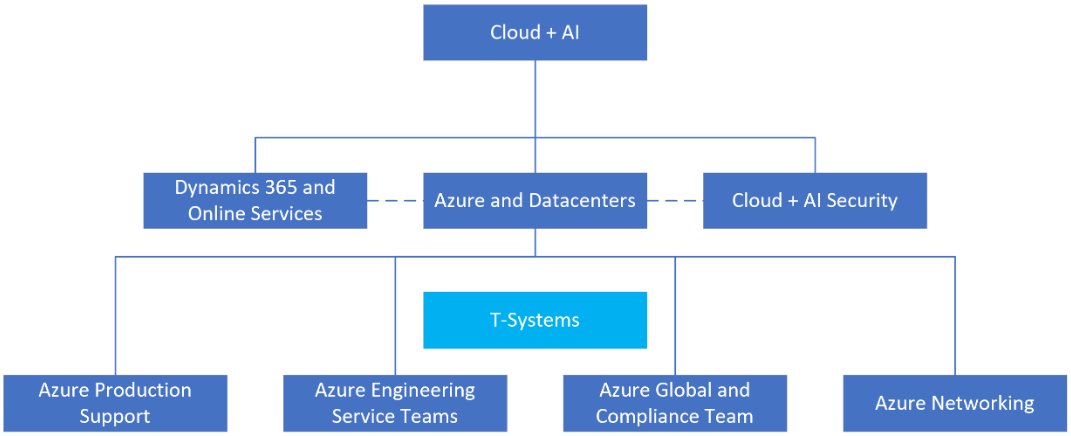
Microsoft does not inspect, approve, or monitor applications that customers deploy to Azure. Moreover, Microsoft does not know what kind of data customers choose to store in Azure. Microsoft does not claim data ownership over the customer information entered into Azure. Azure's Agreement states, "Customers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

Applicable Data Elements

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

People

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



Online Services

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

Cloud + AI Security

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

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

Azure Production Support

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

- **Azure Live Site** - Monitors and supports the Azure platform; proactively addresses potential platform issues; and reacts to incidents and support requests

- **Azure Deployment Engineering** - Builds out new capacity for the Azure platform; and deploys platform and product releases through the release pipeline

- **Azure Customer Support** - Provides support to individual customers and multinational enterprises from basic break-fix support to rapid response support for mission critical applications

Azure Engineering Service Teams

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

- Development of new services
- Serving as an escalation point for support

- Providing operational support for existing services (DevOps model)

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

Global Ecosystem and Compliance Team

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

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

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

Networking

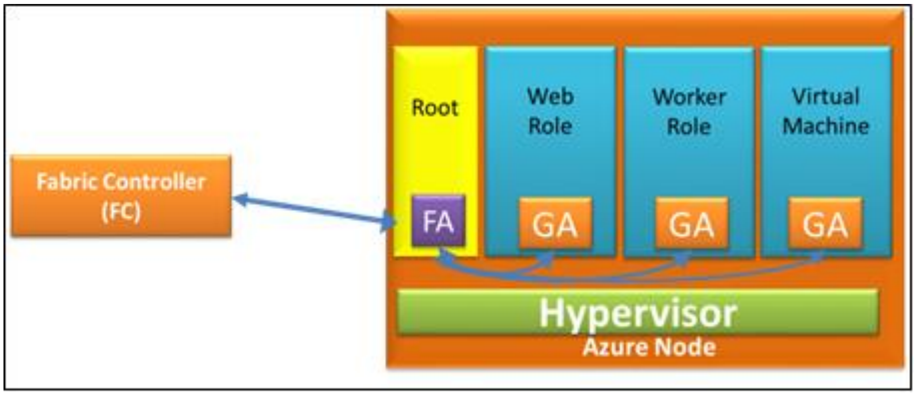
The Networking team is responsible for implementing, monitoring and maintaining the Microsoft network. This team consists of personnel responsible for:

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

Azure Germany Environment

Azure is developed and managed by the Azure and T-Systems teams, 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, called instances, scheduling them on physical CPU cores, assigning them dedicated RAM, and granting and controlling 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 Germany security architecture.



Fabric Controller Lifecycle Management

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

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

FC Managed Operating Systems

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

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

2. **Native OS:** Native OS runs on Azure native tenants such as the FC itself, Azure Storage and Load Balancer that do not have any hypervisor

3. **Guest OS:** Guest OS runs on Guest VMs (for IaaS, FC will run customer provided images on a VHD)

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

Software Development Kits

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

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

Azure Services and Offerings

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

Compute

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

- App Service: API Apps: API Apps enables customers to build and consume Cloud APIs. Customers can connect their preferred version control system to their API Apps, and automatically deploy commits, making code changes.
- App Service: Mobile Apps: Mobile Apps allows customers to accelerate mobile application development by providing a turnkey way to structure storage, authenticate users, and send push notifications. Mobile Apps allows customers to build connected applications for any platform and deliver a consistent experience across devices.
- App Service: Web Apps: Web Apps offers secure and flexible development, deployment and scaling options for web applications of any size. Web Apps enables provisioning a production web application in minutes using a variety of methods including the Azure Portal, PowerShell scripts running on Windows, Command Line Interface (CLI) tools running on any OS, source code control driven deployments, as well as from within the Visual Studio Integrated Development Environment (IDE).

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

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

Cloud Services: Cloud Services is a PaaS service designed to support applications that are scalable, reliable, and inexpensive to operate. Cloud Services is hosted on virtual machines. However, customers have more control over the VMs. Customers can install their own software on VMs that use Cloud Services and access them remotely. It removes the need to manage server infrastructure and lets customers build, deploy, and manage modern applications with web and worker roles. Cloud Services also contains Red Dog Front End (RDFE), which 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 frontend to the Azure Portal and the Service Management API (SMAPI). All requests from the user go through RDFE or Azure Resource Manager.

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

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

Networking

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

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

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

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

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

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

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

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

Storage

Azure Backup: Azure Backup protects Windows client data and shared files and folders on customer's corporate devices. Additionally, it protects Microsoft SharePoint, Exchange, SQL Server, Hyper-V virtual machines, and other applications in the customer's datacenter(s) integrated with System Center Data Protection Manager (DPM). Azure Backup enables customers to protect important data off-site with automated backup to Microsoft Azure. Customers can manage their cloud backups from the tools in Windows Server, Windows Server Essentials, or System Center Data Protection Manager. These tools allow the user to configure, monitor and recover backups to either a local disk or Azure Storage.

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

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

- Blobs: Blobs is Microsoft's object storage solution for the cloud. Blobs can be used to store large amounts of binary data. For example, Blob Storage can be used for an application to store video, or to backup data.

- Disks: A managed or an unmanaged disk is a Virtual Hard Disk (VHD) that is attached to a VM to store application and system data. This allows for a highly durable and available solution while still being simple and scalable.

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

- Queues: Queues is a service for storing large number of messages. Queues provide storage and delivery of messages between one or more applications and roles.

- Tables: Tables provide fast access to large amounts of structured data that do not require complex SQL queries. For example, Tables can be used to create a customer contact application that stores customer profile information and high volumes of user transaction.

- Cool Storage: Cool Storage is a low-cost storage tier for cooler data, where the data is not accessed often. Example use cases for Cool Storage include backups, media content, scientific data, compliance and archival data. Customers can use Cool Storage to retain data that is seldom accessed.

- Premium Storage: Premium Storage delivers high-performance and low-latency storage support for virtual machines with input / output (IO) intensive workloads. Premium Storage is designed for mission-critical production applications.

Databases

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

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

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

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

SQL Server on Virtual Machines: SQL Server on Virtual Machines enables customers to create a SQL Server in the cloud that they can control and manage. SQL Server on Virtual Machines offers a robust infrastructure for SQL Server by using Azure as a hosting environment for enterprise database applications. SQL Server is a database for transactions, queries and analytics for Big Data solutions. SQL Server is not in scope of this SOC report.

Analytics

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

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

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

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

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

AI + Machine Learning

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

Internet of Things

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

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

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

Integration

Service Bus: Service Bus is a multi-tenant cloud messaging service that can be used to send information between applications and services. The asynchronous operations enable flexible, brokered messaging, along with structured first-in, first-out (FIFO) messaging, and publish / subscribe capabilities. Service Bus uses Advanced Message Queuing Protocol (AMQP), Service Bus Messaging Protocol (SBMP), and HTTP as its primary protocols.

Identity

Azure Active Directory (AAD): Azure Active Directory provides identity management and access control for cloud applications. To simplify user access to cloud applications, customers can synchronize on-premises identities, and enable single sign-on. AAD comes in 3 editions: Free, Basic, and Premium. Self-service credentials management is a feature of AAD that allows Azure AD tenant administrators to register for and subsequently reset their passwords without needing to contact Microsoft support. Microsoft Online Directory Services (MSODS) is also a feature of AAD that provides the backend to support authentication and provisioning for AAD.

Management and Governance

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

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

Scheduler: Scheduler lets customers invoke actions that call HTTP/S endpoints or post messages to an Azure Storage queue, Service Bus queue, or Service Bus topic on any schedule. It creates jobs that reliably call services either inside or outside of Azure and run those jobs right away, on a regular or irregular schedule, or at a future date. Scheduler was retired in calendar year Q4 2019 with all of the service functionality moved to Logic Apps, which is not in scope for this SOC report. However, this service continues to support existing customers until it is fully decommissioned.

Security

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

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

Media

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

Internal Supporting Services

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

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

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

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

CEDIS - Active Directory Domain Services: CEDIS - Active Directory Domain Services provides Active Directory Domain Services (AD DS) for internal Microsoft customers like Azure, Online Services, and Microsoft Retail.

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

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

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

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

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

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

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

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

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

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

Workflow: Workflow lets users upload their workflows to Azure and have them executed in a highly scalable manner. This service is currently consumed only by O365 SharePoint Online service.

Microsoft Online Services

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

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

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

Dynamics 365

Dynamics 365 Customer Engagement: Dynamics 365 Customer Engagement is a cloud-based customer relationship management (CRM) business solution that can help customers drive sales productivity and improve the value of marketing efforts through social insights, business intelligence, and campaign management.

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

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

Section IV: Principal Service Commitments and System Requirements

Section IV: Principal Service Commitments and System Requirements

Microsoft makes service commitments to its customers and has established system requirements as part of the Azure service. Some of these commitments are principal to the performance of the service and relate to applicable trust services criteria. Microsoft is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Microsoft's service commitments and system requirements are achieved.

Service commitments to customers are documented and communicated in the Microsoft Online Subscription Agreement, Microsoft Enterprise Enrollment Agreement (Volume Licensing - Online Services Terms), Microsoft Azure Privacy Statement, and Microsoft Trust Center, as well as in the description of the service offering provided online. Service commitments include, but are not limited to, the following:

- Security: Microsoft has made commitments related to securing customer data and complying with relevant laws and regulations. These commitments are addressed through measures including data encryption, authentication mechanisms, physical security and other relevant security controls.

- Availability: Microsoft has made commitments related to percentage uptime and connectivity for Azure as well as commitments related to service credits for instances of downtime.

- Processing Integrity: Microsoft has made commitments related to processing customer actions completely, accurately and timely. These customer actions include, for example, specifying geographic regions for the storage and processing of customer data.

- Confidentiality: Microsoft has made commitments related to maintaining the confidentiality of customers' data through data classification policies, data encryption and other relevant security controls.

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