Deloitte.

Independent Service Auditor's Report

Microsoft Azure

Table of Contents

I. Independent Service Auditor's Report 3

II. Management Assertion - Microsoft Azure Service and Microsoft Cloud Infrastructure and Operations 4

III. Description of Microsoft Azure System 6

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

I. Independent Service Auditor's Report

To: Microsoft Azure

We have examined the effectiveness of Microsoft Azure ("Azure") controls over the security, availability, confidentiality and processing integrity principles of the Azure services during the period January 15, 2015 through July 31, 2015, based on the American Institute of Certified Public Accountants (AICPA) and Chartered Professional Accountants of Canada (CPA Canada) trust services security, availability, confidentiality and processing integrity criteria. Azure's management is responsible for maintaining the effectiveness of these controls. Our responsibility is to express an opinion based on our examination. Microsoft Cloud Infrastructure and Operations (MCIO) is an internal service organization that provides computer processing services to Azure. Azure's description includes a description of MCIO's computer processing services used by Azure to process transactions for its user entities.

Our examination was conducted in accordance with attestation standards established by the AICPA, and accordingly, included (1) obtaining an understanding of the controls related to the security, availability, confidentiality and processing integrity principles of the Azure services, (2) testing and evaluating the operating effectiveness of Azure's controls, and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of the nature and inherent limitations of controls, Azure's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent or detect and correct error or fraud, unauthorized access to systems and information, and failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

In our opinion, Azure maintained, in all material respects, effective controls over the security, availability, confidentiality and processing integrity principles of the Azure services during the period January 15, 2015 through July 31, 2015 to provide reasonable assurance that:

- the system was protected against unauthorized access, use or modification,
- the system was available for operation and use as committed or agreed,
- information within the system, designated as confidential, was protected as committed or agreed, and
- the system processing was complete, valid, accurate, timely, and authorized

based on the AICPA and CPA Canada trust services security, availability, confidentiality and processing integrity criteria.

Deloitte & Touche LLP

November 19, 2015

Seattle, WA

II. Management Assertion - Microsoft Azure Service and Microsoft Cloud Infrastructure and Operations

Assertion by Management of Microsoft Azure Service Organization regarding its Azure System for the period January 15, 2015 to July 31, 2015.

Management Assertion Regarding the Effectiveness of its Controls

Microsoft Azure maintained effective controls over the security, availability, confidentiality and processing integrity of the Azure services, as defined by the following Systems / Services Description, during the period January 15, 2015 to July 31, 2015[1], to provide reasonable assurance that:

- the system was protected against unauthorized access, use or modification,
- the system was available for operation and use as committed or agreed,
- information within the system, designated as confidential, was protected as committed or agreed, and
- the system processing was complete, valid, accurate, timely, and authorized

based on the AICPA and CPA Canada trust services security, availability, confidentiality and processing integrity criteria, which are available at www.webtrust.org.

The following Systems / Services Description of the Azure environment identifies the aspects of the Azure services covered by this assertion.

Microsoft Azure

November 19, 2015

[1] Controls were placed into operation from April 15, 2015 for following Microsoft Azure services: Backend Health Management, ExpressRoute, Redis Cache, Scheduler, ARM, API Management, IAM - ADUXP/ IAMUX / SF / SSO / SSGM, ADGateway, evoSTS, Automation, SQL Database, SQL VM, HDInsight and dSTS.

Assertion by Management of Microsoft Cloud Infrastructure and Operations regarding Microsoft Azure System for the period January 15, 2015 to July 31, 2015.

Management Assertion Regarding the Effectiveness of its Controls

Microsoft Cloud Infrastructure and Operations (MCIO) maintained effective controls over the security, availability, confidentiality and processing integrity of the of the MCIO Information Technology ("IT") Infrastructure and Services relevant to the Azure services, as defined by the following Systems / Services Description, during the period January 15, 2015 to July 31, 2015, to provide reasonable assurance that:

- the system was protected against unauthorized access, use or modification,
- the system was available for operation and use as committed or agreed,
- information within the system, designated as confidential, was protected as committed or agreed, and
- the system processing was complete, valid, accurate, timely, and authorized

based on the AICPA and CPA Canada trust services security, availability, confidentiality and processing integrity criteria, which are available at www.webtrust.org.

The following Systems / Services Description of the Azure environment identifies the aspects of the MCIO IT infrastructure and services covered by this assertion.

Microsoft Cloud Infrastructure and Operations

November 19, 2015

III. Description of Microsoft Azure System

Overview of Operations

Business Description

Azure is a cloud computing platform and infrastructure for building, deploying and managing applications and services 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) and enables hybrid solutions that integrate cloud services with customers' on-premises resources.

Azure supports many customers, partners, and government organizations that span a broad range of products and services, geographies and industries. Azure is designed to meet their security, privacy, and compliance requirements.

Report Scope Boundary

This report covers the following Azure features including infrastructure, development, operations, and support for Cloud Services, as well as infrastructure for Office 365:

1. **Compute Services**
    a. Virtual Machines (including those with SQL Server)
    b. Cloud Services (includes stateless Web and Worker roles)
    c. Batch
    d. Fabric
    e. Red Dog Front End (RDFE)
    f. Azure Management Portal (AUX)
    g. Service Management Application Programming Interface (SMAPI)
2. **Web & Mobile**
    a. Mobile Services
    b. Web Apps (formerly known as Azure Websites)
    c. API Management
    d. Notification Hubs
    e. Workflow
3. **Data & Storage**
    a. SQL Database
    b. Redis Cache
    c. Storage (includes blobs, queues and tables)
    d. Storage Premium

4. **Analytics**
    a. HDInsight
    b. Event Hubs
5. **Internet of Things**
    a. Event Hubs
    b. Notification Hubs
6. **Networking**
    a. Virtual Network
    b. ExpressRoute
    c. Traffic Manager
    d. Load Balancer
7. **Media & CDN**
    a. Media Services
8. **Hybrid Integration**
    a. Service Bus
9. **Identity & Access Management**
    a. Azure Active Directory
        i. Microsoft Directory Services and Organizational Identity
        ii. Access Control Service (ACS)
        iii. Identity and Access Management - Self-Service Password Reset (SSPR)
        iv. Identity and Access Management - Cloud Password Single Sign-On (SSO)
        v. Identity and Access Management - Self-Service Group Management (SSGM)
        vi. Identity and Access Management - Sync Fabric (SF)
    b. Rights Management Service (RMS)
    c. Multi-Factor Authentication (MFA)
10. **Management**
    a. Scheduler
    b. Automation
    c. Intune

Locations Covered by this Report

Azure production infrastructure is located in globally distributed datacenters that are managed by MCIO. MCIO is responsible for the physical security of the Azure datacenters, data protection, and physical hardware asset management and network services.

The datacenters in scope for the purposes of this report are:

- North America
    - East Central U.S. - Boydton, VA
    - East Central U.S. - Ashburn, VA
    - East Central U.S. - Bristow, VA
    - East Central U.S. - Reston, VA
    - South Central U.S. - San Antonio, TX
    - North Central U.S. - Chicago, IL
    - North Central U.S. - West Des Moines, IA
    - Western U.S. - Quincy, WA
    - Western U.S. - Santa Clara, CA
- Europe
    - Western Europe - Amsterdam, Netherlands
    - Western Europe - Dublin, Ireland
- Asia
    - East Asia - Hong Kong, China
    - South East Asia - Singapore
    - Western Japan - Osaka, Japan
    - Western Japan - Osaka City, Japan
    - Eastern Japan - Saitama, Japan
    - East Asia Pacific - Tokyo, Japan
    - Western Australia - Macquarie Park, Australia
    - Eastern Australia - Melbourne, Australia
- South America
    - South Brazil - Campinas, Brazil

People

Azure is comprised of the following groups who support in the delivery and management of these cloud based services:

Azure Production Support

The Azure Production Support Team is responsible for build out, deployment and management of Azure services. This team consists of Live Site monitoring, Deployment Engineering and Customer Support.

Azure Engineering Feature Teams

The Azure Engineering Feature Teams manage the component lifecycle including development of new features, escalation point for support and operational support for existing features (DevOps model).

Global Ecosystem and Compliance Team

The Azure Global Ecosystem and Compliance 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 and internal and external audit coordination.

Cloud and Enterprise Security Team

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 across Azure. The Cloud and Enterprise Security team is involved in the review of all deployments and enhancements of Azure features to facilitate security considerations at every level of the Secure Development Lifecycle (SDL).

Azure Environment

Azure is developed and managed by the Azure team, and is part of Microsoft Cloud and Enterprise (C&E), which provides the platform layer. MCIO provides the physical infrastructure on which the Azure platform runs and data is stored. Customers provide and manage the applications and data that sit on the platform.

Services and Software Overview

Azure provides a platform where customers, users, and applications can interact.

Azure Management Portal

Azure Management Portal (AUX) is an administrative portal for managing customer accounts and deploying, managing, and monitoring their hosted services.

Red Dog Front End

RDFE is the communication path from the user to the fabric. RDFE is the publicly exposed API which is the front end to the Management Portal and the Service Management API (i.e., Visual Studio, Azure, etc.).

Azure Portal and Service Management APIs

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 Portal and Service Management APIs (SMAPIs), and are authenticated by their Microsoft Accounts or Organizational Accounts.

Microsoft Online Services Customer Portal and Microsoft Accounts / Organizational Account

Users who have access to Azure customer applications have established authentication and authorization privileges based on their Microsoft Accounts (MSA) and / or Organizational Accounts. Azure customer billing is handled by Microsoft Online Services Customer Portal (MOCP).

Azure Infrastructure

Azure Core Infrastructure Details

Azure Node Detail

The collection of Azure Hypervisor, Root Operating Systems, Fabric Agent, Customer Virtual Machines (VMs), and Guest Agents make up the Azure Node.

Fabric Controller Lifecycle Management

In Azure, VMs run on groups of physical servers (nodes) 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.

FC Managed Operating Systems

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

- **Host OS:** Host OS is a customized version of the Windows OS that runs on Host Machine Root VMs
- **Native OS:** Native OS runs on Azure native tenants such as RDFE that do not have any hypervisor
- **Guest OS:** Guest OS runs on Guest VMs (for IaaS, FC will run customer provided images on a VHD)

Software Development Kits

Azure is a Windows Server-based environment that allows customers to create Azure applications in many development languages. Microsoft provides language-specific Software Development Kits (SDKs) today for .NET, Java, PHP, Ruby and Node.js. Additionally, 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.

Compute Services

Azure Virtual Machines

Azure VMs is an IaaS feature that provides customers with the ability to deploy and run VMs with Windows Server and Linux Operating Systems enabling customers to migrate their workloads to the Azure cloud without a need to change existing code.

SQL Virtual Machines

A SQL VM enables customers to create a SQL server in the cloud that they control and manage. SQL VMs offer a robust infrastructure for SQL Server by using Azure as a hosting environment of enterprise database applications.

Cloud Services

Azure Cloud Services allows customers to create highly available and scalable applications and services using the PaaS environment. Customers upload applications and Azure manages the deployment details.

Batch

Azure Batch provides a foundational platform service for application developers with application requirements to perform large-scale compute; it manages the large numbers of virtual machines on which the workloads are executed and provides the job scheduling capabilities which allocate workload tasks to the virtual machines for execution.

Web & Mobile

Mobile Services

Mobile Services allows customers to accelerate mobile application development by providing a turnkey way to structure storage, authenticate users, and send push notifications. Mobile Services allows customers to build connected applications for any platform and deliver a consistent experience across devices.

Web Apps

Azure Web Apps is a highly scalable web hosting service for public and private clouds that is optimized for cloud hosting economics and is integrated with popular Operations Support System (OSS) web apps, frameworks, and tools. Azure Web Apps offers secure and flexible development, deployment and scaling options for any sized web application.

API Management services

API Management helps customers understand application usage, health, latency, activity and trends as well as manage application lifecycle, versioning, monitoring, caching, and alerting. It also protects the customer's backend with authorization, quotas, rate limits and provides request validation. API providers can expose their backend API to application developers through Azure API Management services.

Notification Hubs

Azure Notification Hubs provide an infrastructure that enables users to send mobile push notifications from any backend (in the cloud or on-premises) to any mobile platform. Notification Hubs is a multi-tenant service for connecting applications through the cloud. Notification Hubs can be used for both enterprise and consumer scenarios.

Workflow

The Azure Workflow service provides a high-scale, high-density environment where workflows authored by customers in the Office365 platform can execute. SharePoint Online allows workflows to be created that are attached to SharePoint sites or lists. Using this, customers can automate numerous human and document management processes.

Data & Storage

SQL Database

Azure SQL Database provides all of the key features of a relational database management system, including atomic transactions, concurrent data access by multiple users with data integrity, ANSI SQL queries, and a familiar programming model. Like SQL Server, SQL Database can be accessed using ADO.NET Entity Framework, JDBC, and PHP. SQL Database also provides a federation option that distributes data across multiple servers.

Redis Cache

Redis Cache is an open source implementation of an in-memory cache server. A cache service allows quick access to frequently requested data. Redis Cache handles the management aspects of the cache instances, providing customers with replication of data, fail-over, and connecting to the Cache using Secure Sockets Layer (SSL) support, etc.

Storage

The Storage service for Azure provides distributed persistent storage and three different data storage types: blobs, tables, and queues. 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.

Storage Premium

Premium Storage delivers high-performance, low-latency disk support for I/O intensive workloads running on Azure Virtual Machines. 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.

Analytics

HDInsight

HDInsight is a 100% Hadoop cloud service. It allows users to store, process and analyze terabytes or petabytes of unstructured and semi-structured data. HDInsight uses blob storage to hold files and log, clickstream, device, and sensor telemetry data.

Event Hubs

Event Hubs is a feature of Service Bus. It is an event and telemetry ingress service that can be used for common application and user workflow monitoring. Event Hubs provides provisioning of capacity to process events from millions of event publishers while preserving event order on a per-device basis.

Internet of Things

Event Hubs

Please see above under Analytics section

Notification Hubs

Please see above under Web & Mobile section

Networking

Virtual Network

Azure Virtual Network enables customers to create a logically isolated section in Azure and securely connect to their on-premises datacenter or a single client machine using an IPsec connection. Virtual Network makes it easy to take advantage of Azure's scalable, on-demand infrastructure while providing connectivity to data and applications on-premises, including systems running on Windows Server, mainframes and UNIX. Virtual Network enables customers to extend their datacenter, build distributed applications and remotely debug applications.

ExpressRoute

Azure ExpressRoute enables customers to extend their on-premises networks into Azure over a dedicated private connection facilitated by a connectivity partner. Connectivity can be from any-to-any (IP VPN) network, a point-to-point Ethernet network, or a virtual cross-connection through a connectivity provider at a co-location facility.

Traffic Manager

Azure Traffic Manager allows you to control distribution of user traffic to your specified endpoints, which can include Azure Cloud services, websites and other endpoints. Traffic Manager applies an

intelligent policy engine to Domain Name Service (DNS) queries for the domain names of your Internet resources.

Load Balancer

Azure Load Balancer is an infrastructure component that provides load balancing capabilities to internal components as well as to external customers who want to add high availability and capacity to their applications. Azure Load Balancer distributes incoming traffic load among healthy service instances in cloud services or VMs defined in a load balancer set. It can be used for TCP/UDP-based protocols such as HTTP, HTTPS, SMTP as well as protocols used for real-time voice, video messaging applications.

Media

Media Services

Azure Media Services provides customers a PaaS layer for managing media workflows in Azure through Media Encoding and Media Streaming. Media Encoding enables customers to upload their raw mezzanine content to Azure Storage and trigger media processing jobs. Media Streaming enables customers to deliver media for consumption by end users.

Hybrid Integration

Service Bus

Service Bus provides a multi-tenant service for connecting applications through the cloud. It provides a hosted, secure, and widely available infrastructure for widespread communication, large-scale event distribution, naming, and service publishing.

Identity & Access Management

Azure Active Directory

Microsoft Online Directory Services

Azure Active Directory is a modern, REST-based service that provides identity management and access control capabilities for cloud applications. It enables one identity service across Azure, Microsoft Office 365, Microsoft Dynamics CRM Online, Microsoft Intune and other third-party cloud services.

Federated Sync - The Federated Service Synchronization web service enables federated services to synchronize identity, address book, and licensed capability assignments from the Microsoft Online Directory Service (MSODS, or simply DS) and to publish provisioning-related state back to the DS.

Directory Synchronization (DirSync) - Directory sync is a foundational and critical scenario of the identity and access management solution used for integrating with Azure Active Directory. DirSync enables customers to manage the entire lifecycle of their cloud user and group accounts using their on-premises Active Directory management tools.

Organizational Identity

Organizational Identity (OrgID) is the identity provider for Azure Active Directory providing authentication services for identities owned by enterprise customers of Microsoft's cloud services, including Azure and Office 365.

Evolved Security Token Service

Evolved Security Token Service (evoSTS) is an Azure web service role built for identity and federation providing a stateless service that accesses multiple principal and key stores. evoSTS absorbs the roles of multiple STSs, so that partners see one AAD STS.

Access Control Service

ACS is a cloud-based service that provides an easy way 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.

Identity and Access Management - Self Service Password Reset

The IAM SSPR services are cloud-based services that allow the Azure Active Directory tenant administrators to register for and subsequently reset their passwords without contacting Microsoft support.

Identity and Access Management - Cloud Password Single Sign On

The IAM - SSO is the ability for customers to use a single set of credentials to access both on-premises and online resources.

Identity and Access Management - Self Service Group Management

The IAM - SSGM service supports group object create, read, update, and delete (CRUD) operations through Graph API. The Azure Active Directory 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.

Identity and Access Management - Sync Fabric

IAM - SF enables the automatic creation, management and removal of user identities in SaaS applications by connecting to provisioning endpoints provided by application vendors.

Rights Management Services

Azure RMS helps protect organization's sensitive information from unauthorized access, and controls how this information is used. Rights Management uses encryption, identity, and authorization policies to help protect files and email.

Multi-Factor Authentication

Azure MFA helps safeguard access to data and applications while addressing user demand for a simple sign-on process. Offering enhanced protection from malware threats, and real-time alerts notifying Information Technology (IT) departments of potentially compromised account credentials,

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.

Management

Scheduler

Scheduler is a high availability service that enables customers to create jobs that can invoke an HTTP endpoint or post a message to an Azure Storage queue on a regular interval or on a prescribed schedule.

Automation

Azure Automation service provides customers a fully managed, multi-tenant, PaaS layer for automating daily processes and reducing error-prone manual activities. Customers can orchestrate their end-to-end workflows, as well as integrate with many systems in Azure.

Intune

Intune is a cloud-based service for Mobile Device Management (MDM) of Windows, iOS, and Android mobile devices. It can be used alone or integrated with System Center 2012 R2 Configuration Manager to extend management capabilities.

Azure Services Supporting Infrastructure

Physical Network

The Azure Physical Network (PhyNet) infrastructure is used to provide all datacenter connectivity for all Azure capacity: Compute, Storage, etc. The physical network infrastructure is completely transparent to Azure customers.

DNS

The Azure supporting DNS service hosts critical domains belonging to the Azure platform, as opposed to the customers' domains. The IDNS service offers hostname to Dedicated Internet Protocol (DIP) resolution within the customers' VNET. Recursive resolvers are used to provide DNS resolution capabilities to Azure VMs and infrastructure.

Active Directory Gateway

The Active Directory Gateway (ADGateway) is an Azure web service which acts as a stateless front door / reverse proxy for all requests to other services in Azure Active Directory.

Identity and Access Management - User Interface

Identity and Access Management - User Interface (ADUXP) serves as the core data layer which serves the Azure Portal Administrator UX, as well as portions of the Information Worker UX.

Identity and Access Management - User Experience

Identity and Access Management - User Experience (IAMUX) is a simple web service that hosts various pages that information workers interact with to perform daily tasks like managing their profile, changing their passwords, and the like.

Azure Resource Manager

Azure Resource Manager (ARM) is a collection of capabilities that enables the deployment and management of resources in Azure.

Datacenter Security Token Service

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

Jumpboxes

Jumpboxes are used by Azure service teams to operate Azure services and allow access to and from Azure datacenters. They function as utility servers for runners, deployments, and debugging; building out new clusters; managing certificates; and, collecting diagnostics information from production systems.

Backend Health Management

The Backend Health Management platform is available to first party customers for management of hyper-scale services used in high-availability scenarios.

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.

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, "Except for Software we license to you, as between the parties, you retain all right, title and interest in and to Customer Data. We acquire no rights in Customer Data, other than the right to host Customer Data on Microsoft systems, including the right to use and reproduce Customer Data within Microsoft systems solely for such hosting purposes."