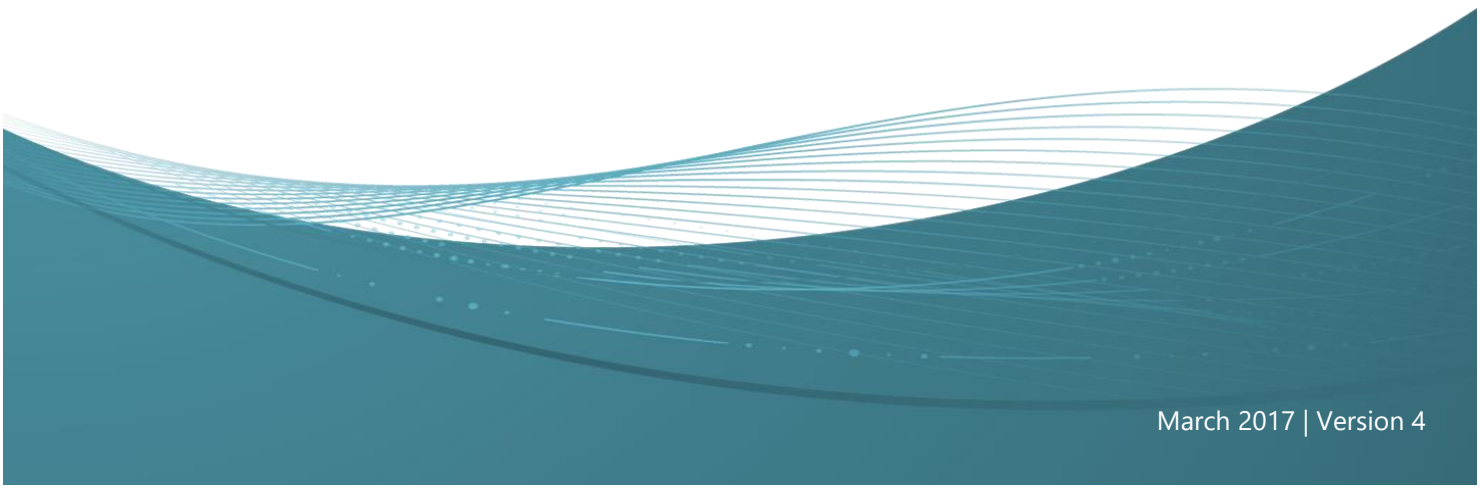
Standard Response to Request for Information

Microsoft Azure Security, Privacy, and Compliance



March 2017 | Version 4

Abstract

This response document helps address standard Requests for Information (RFI) with which we empower customers to evaluate different offerings in the market place today. Through the mappings available in the CCM, we can illustrate how Azure has implemented security and privacy controls aligned to other international standards such as ISO/IEC 27001, US Government frameworks including FedRAMP, and industry certifications such as PCI DSS.

Change Log

Version	Date	Contributor	Reviewed by
3	October 2015	Joel Sloss	Frank Simorjay
4	March 2017	Abhishek Pradhan Eric Tierling	Joel Sloss

Disclaimer

Contents

Introduction

The Cloud Security Alliance (CSA) is a not-for-profit organization promoting the use of best practices for security assurance within cloud computing.

The CSA published the Cloud Control Matrix to support customers in the evaluation of cloud providers and to identify questions prudent to have answered before moving to cloud services. In response, Microsoft Azure has created this document to outline how we meet the suggested principles.

Learn more:
https://cloudsecurityalliance.org

Global adoption of cloud services continues to accelerate, yet many organizations remain wary of trusting multi-tenant platforms with their data, applications, or infrastructure. At Microsoft, trust is a focal-point for services delivery, contractual commitments, and industry accreditation.

To help establish this trust, Microsoft Azure operates services according to three fundamental tenets:

- **Experience** that facilitates innovation and the development of reliable software and services that customers can use to build their own secure, private, and compliant solutions.
- **Transparency** that provides insight into how Microsoft achieves security and privacy for its customers and meets compliance standards.
- **Shared responsibility** that helps ensure both individuals and organizations can manage their cloud computing experiences in accordance with their security and privacy needs.

Azure is hosted in Microsoft datacenters around the world, and is designed to offer the performance, scalability, security, and service levels that enterprise customers expect. We have applied state-of-the-art technology and processes to maintain consistent and reliable access, security, and privacy for every user. Azure has built-in capabilities for compliance with a wide range of regulations and privacy mandates.

Microsoft Azure is a growing collection of integrated cloud services—analytics, computing, database, mobile, networking, storage, and web—for moving faster, achieving more, and saving money. Azure serves as a development, service hosting, and service management environment, providing customers with on-demand compute, storage, networking, and content delivery capabilities to host, scale, and manage applications on the Internet.

In order to get the most out of this framework, readers should be familiar with basic Azure and cloud computing concepts, as well as security and compliance fundamentals—they will not be covered here. Links to additional materials can be found here: https://azure.microsoft.com/en-us/get-started/, as well as through the Azure Trust Center.

Experience

Microsoft has considerable experience in delivering consumer and enterprise cloud services at global scale. Since the launch of MSN in 1994, Microsoft's cloud infrastructure has grown to support more than one billion customers and 200 million organizations in 76 markets worldwide. Microsoft uses the knowledge it gains by operating its own cloud infrastructure and by providing its customers with cloud-based solutions to develop best practices and technology innovations that support optimized security, privacy, compliance, and reliability.

Microsoft enables organizations to adopt cloud computing rapidly via its cloud services such as Azure, Office 365, and Microsoft Dynamics 365 and takes an industry-leading approach to security, privacy, and reliability.

Transparency

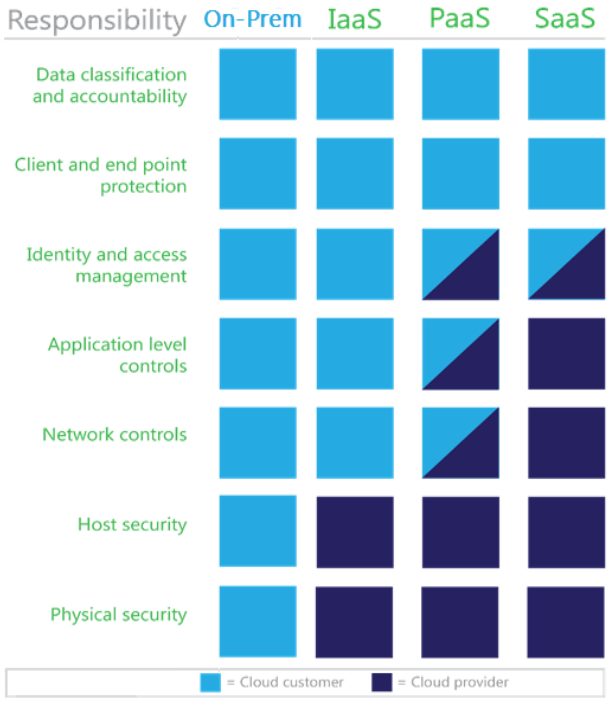
Microsoft is committed to transparency and openness in all aspects of its cloud services. It shares details about its efforts in the areas of security and privacy through several portals and reports, including:

- **Microsoft Trust Centers**, which are used to address key issues and concerns expressed by Microsoft customers about specific Microsoft services. Trust Centers have been established for Office 365, Microsoft Azure , Microsoft Dynamics 365, and Microsoft Intune.
- **Law Enforcement Requests Report**. In March of 2013, Microsoft began publishing the number of demands it receives from law enforcement agencies as well as how many entities may be affected by such demands.
- **Cloud Security Alliance.** Microsoft is committed to transparency through its work with and support for CSA, who launched the Security, Trust & Assurance Registry (STAR) initiative in 2011 to promote transparency in cloud computing.

Shared Responsibilities

Microsoft understands how different cloud service models affect the ways that responsibilities are shared between cloud service providers (CSP) and customers.

The three primary cloud service models are infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). The left-most column in the following figure shows seven responsibilities, all of which contribute to the overall security, privacy, and reliability of cloud computing environments. Two of the responsibilities are solely in the domain of customers, and two other responsibilities are in the domain of cloud providers. The remaining three responsibilities are shared between customers and cloud providers, depending on which cloud service model is being used.



The figure shows how customers and providers share the identity and access management responsibility for both Office 365, Dynamics 365 (a SaaS offering) and Azure (an IaaS/PaaS offering). It also shows how customers and providers share the application-level controls and network controls for Azure, but that these responsibilities fall completely in the domain of the provider for SaaS services such as Office 365 & Dynamics 365.

The Microsoft Azure Trust Center offers additional information on topics such as the Online Service Terms, Privacy Statement, Security Overview, and Terms of Use.

To learn more, visit:

https://azure.microsoft.com/en-us/support/trust-center/

Scope

This document provides our customers with a detailed assessment of how Azure core services fulfill the security, privacy, compliance, and risk management requirements as defined in the Cloud Security Alliance (CSA) Cloud Control Matrix (CCM) version 3.0.1. Note, however, that the responses below are intended to provide information on how Microsoft operates Azure services; customers have accountability to control and maintain their cloud environment once the service has been provisioned (for example, user access management with appropriate policies and procedures in accordance with regulatory requirements).

Azure's CCM responses are scoped to Azure services in alignment with our ISO/IEC 27001 and PCI DSS attestations, including Microsoft's physical datacenters:

- Compute (Virtual Machines, Cloud Services, RemoteApp)
- Web and Mobile (App Service, Mobile Apps, API Management)
- Data and Storage (SQL Database, Storage, StorSimple)
- Analytics (HDInsight, Data Factory)
- Networking (Virtual Networks)
- Hybrid Integration (BizTalk Services, Service Bus, Backup, Site Recovery)
- Identity and Access Management (Azure Active Directory, Multi-Factor Authentication)
- Developer Services (Visual Studio Online)
- Management (Preview Portal, Scheduler, Key Vault)

Azure Common Controls

Organizations looking to adopt cloud services should look for a set of common controls and control details that address issues with the adoption of cloud and cloud-specific risks.

However, the CSP selection exercise frequently takes place in a climate of intense business pressure to reduce costs and increase flexibility; here, a drawn-out risk management process may be seen as an inhibitor, rather than an enabler, of business goals.

Best Practices

Some of the unease and complexity involved in selecting a cloud provider can be alleviated by using a common controls framework. Such a framework should consider not only best practices in information security, but also cloud-specific deployment considerations and risks. In addition, such a framework should address much of the cost involved in the evaluation of alternate solutions and help to significantly manage risk that must otherwise be considered.

Complexity

A cloud-specific controls framework such as the Cloud Control Matrix (CCM) reduces the risk of an organization failing to consider important factors when selecting a cloud provider. The risk is further mitigated by relying on the cumulative knowledge of industry experts who created the framework, and taking advantage of the efforts of many

The fact that Azure services are certified to ISO/IEC 27001 means that we have been able to meet the external auditors' expectations that our environment meets or exceeds such standards.

The public copy of the Azure ISO Certification is available here:

https://azure.microsoft.com/en-us/support/trust-center/compliance/iso27001/

organizations, groups, and experts in a thoughtfully laid-out form. In addition, an effective industry framework will be regularly updated to take into account the changes in maturing technologies, based on the experiences of experts who have reviewed many different approaches.

Comparison

For organizations that do not have detailed knowledge about the different ways that cloud providers can develop or configure their offerings, reviewing a fully developed framework can provide insight into how to compare similar offerings and distinguish between providers. A framework can also help determine whether a specific service offering meets or exceeds compliance requirements and/or relevant standards.

Azure's Approach

Both Azure and the underlying Microsoft Cloud and Infrastructure Operations (MCIO) physical environments employ security frameworks that span multiple standards, including the ISO 27000 family of standards, NIST 800, and others.

Our security framework, based on ISO/IEC 27001 and ISO/IEC 27018, enables customers to evaluate how Microsoft meets or exceeds its security standards and implementation guidelines. ISO/IEC 27001 defines how to implement, monitor, maintain, and continually improve the Information Security Management System (ISMS).

The Microsoft Security Policy also aligns with ISO/IEC 27002, augmented with requirements specific to Azure. ISO/IEC 27002 is not a certification but provides a suggested set of suitable controls for the Information Security Management System as described in ISO/IEC 27001.

How to Read: CSA Requirements and Microsoft's Response

On the following pages, we have mapped our security practices to the guidance provided by the CCM. The first two columns, headed "Control ID in CCM" and "Control Description", consist of content directly from the CCM identifying relevant controls. The third column, headed "Microsoft Azure Response", consists of short explanations of how Azure controls satisfy the CSA recommendations.

In previous versions of this document, we placed references to the ISO/IEC 27001 controls attested to by the MCIO and/or Azure ISO/IEC 27001 certifications. However, since the CCM provides direct mappings in the public framework to ISO, PCI, FedRAMP, and many other standards, we now recommend that customers refer to that framework for the equivalent ISO controls. Azure's responses to the CCM here are complete in the context of the guidance requested.

More Information and Guidance

A review of the ISO/IEC 27001 and ISO/IEC 27002 publicly available standards is highly recommended. ISO Standards are available for purchase at the International Organization for Standardization website: http://www.iso.org/iso/iso_catalogue. These ISO standards provide deep detail and guidance.

Microsoft Azure Responses to CSA CCM v3.0.1

Application and Interface Security: Controls AIS-01 through AIS-04		
Control ID in CCM[1]	**Control Description (CCM Version 3.0.1, Final)**	**Microsoft Azure Response**
AIS-01: Application & Interface Security - Application Security	*Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.*	The Microsoft Azure trustworthy foundation concept ensures application security through a process of continuous security improvement with its Security Development Lifecycle (SDL) and Operational Security Assurance (OSA) programs using both Prevent Breach and Assume Breach security postures. Prevent Breach works through the use of ongoing threat modeling, code review and security testing; Assume Breach employs Red-Team / Blue-Team exercises, live site penetration testing and centralized security logging and monitoring to identify and address potential gaps, test security response plans, reduce exposure to attack and reduce access from a compromised system, periodic post-breach assessment and clean state. Azure validates services using third party penetration testing based upon the OWASP (Open Web Application Security Project) top ten and CREST-certified testers. The outputs of testing are tracked through the risk register, which is audited and reviewed on a regular basis to ensure compliance to Microsoft security practices.
AIS-02: Application & Interface Security - Customer Access Requirements	*Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.*	Microsoft's customer access controls and trust levels are described on the Microsoft Azure Trust Center website. Before using Azure Services, customers are required to review and agree with the acceptable use of data and the Microsoft Azure service, as well as security and privacy requirements, which are defined in the Microsoft Online Services Use Rights, Microsoft Online Subscription Agreement, Microsoft Azure Platform Privacy Statement and Technical Overview of the Security Features in Microsoft Azure Platform. Microsoft was the first major cloud service provider to make contractual privacy commitments (as well as to incorporate the best practices encompassed by ISO/IEC 27018) that help assure the privacy protections built into in-scope Azure services are strong. Among the commitments that Microsoft supports are: EU Model Clauses EU data protection law regulates the transfer of EU customer personal data to countries outside the European Economic

[1] CCM content in columns 1 and 2 is © 2015 Cloud Security Alliance, used with permission.

		Area (EEA). Microsoft offers customers the EU Standard Contractual Clauses that provide specific contractual guarantees around transfers of personal data for in-scope services. Europe's privacy regulators have determined that the contractual privacy protections Azure delivers to its enterprise cloud customers meet current EU standards for international transfers of data. Microsoft is the first cloud provider to receive this recognition. US-EU Safe Harbor Framework and the US-Swiss Safe Harbor Program Microsoft abides by these frameworks set forth by the US Department of Commerce regarding the collection, use, and retention of data from the EEA and Switzerland.
AIS-03: Application & Interface Security - Data Integrity	*Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.*	Microsoft Azure defines acceptable standards to ensure that data inputs to application systems are accurate and within the expected range of values. Where appropriate, data inputs should be sanitized or otherwise rendered safe before being inputted to an application system. Developers follow Microsoft's SDL methodology which includes requirements for data input and output validation checks. Additional information can be found here: http://www.microsoft.com/en-us/sdl/. Internal processing controls are implemented within the Microsoft Azure environment in order to limit the risks of processing errors. Internal processing controls exist in applications, as well as in the processing environment. Examples of internal processing controls include, but are not limited to, the use of hash totals, and checksums.
AIS-04: Application & Interface Security - Data Security / Integrity	*Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity and availability) across multiple system interfaces, jurisdictions and business functions to prevent improper disclosure, alteration, or destruction.*	Microsoft maintains and regularly updates the Azure Information Security Management Policy and information security guidelines, standard operating procedures for data security, and contractual commitments to international data protection directives which apply across Azure services. In addition, Microsoft Azure software updates are reviewed for unauthorized changes through Security Development Lifecycle (SDL) change and release management processes. Automated mechanisms are used to perform periodic (at least every hour) integrity scans and detect system anomalies or unauthorized changes. Microsoft applies SDL to design, develop, and implement Microsoft Azure services. SDL helps to ensure that communication and collaboration services are highly secure, even at the foundation level, and align with other industry standards including FedRAMP, ISO, and NIST.

Audit Assurance and Compliance: Controls AAC-01 through AAC-03		
AAC-01: Audit Assurance & Compliance - Audit Planning	*Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.*	Microsoft Azure independent audit reports and certifications are shared with customers in the format native to the type of audit. These certifications and attestations accurately represent how we obtain and meet our security and compliance objectives and serve as a practical mechanism to validate our promises for customers.
AAC-02: Audit Assurance & Compliance - Independent Audits	*Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.*	SOC, ISO/IEC 27001 certifications and other audit reports for Microsoft Azure and Microsoft Cloud Infrastructure and Operations (global datacenters) can be found on the Azure Trust Center website (http://azure.microsoft.com/trustcenter) and the website of our external ISO auditor, the BSI Group. Additional audit information is available under NDA upon request by prospective and existing customers through their Microsoft Account Representative. Applicable audits of Azure infrastructure and platform services are carried out at least annually by certified independent assessors, including SOC 1 / 2, ISO/IEC 27001, FedRAMP, PCI, CDSA, and others.
AAC-03: Audit Assurance & Compliance - Information System Regulatory Mapping	*Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.*	Microsoft Azure has designed and implemented an Information Security Management System (ISMS) framework that addresses industry best-practices for information security and privacy. The ISMS has been documented and communicated in a customer-facing Microsoft Security Policy, which can be made available upon request (customers and prospective customers must have a signed NDA or equivalent in place to receive a copy). Microsoft Azure performs annual ISMS reviews, the results of which are reviewed by security and compliance management. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions. Microsoft Azure has implemented a common controls framework which maps and aligns control domains and activities across services, requirements, and operations for each audit and certification. This mechanism is regularly maintained and updated with new controls when new services or standards are incorporated into Microsoft's continuous cloud compliance program. Additional detail on Microsoft's ISMS can be found at http://download.microsoft.com/download/A/0/3/A03FD8F0-6106-4E64-BB26-13C87203A763/Information_Security_Management_System_for_Microsofts_Cloud_Infrastructure.pdf.

Business Continuity Management and Operational Resilience: Controls BCR-01 through BCR-11		
BCR-01: Business Continuity Management & Operational Resilience - Business Continuity Planning	*A consistent unified framework for business continuity planning and plan development shall be established, documented and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following:* • *Defined purpose and scope, aligned with relevant dependencies* • *Accessible to and understood by those who will use them* • *Owned by a named person(s) who is responsible for their review, update, and approval* • *Defined lines of communication, roles, and responsibilities* • *Detailed recovery procedures, manual work-around, and reference information* • *Method for plan invocation*	Management has established roles and responsibilities to oversee implementation of the Microsoft Security Policy and operational continuity across Azure. Microsoft Azure management is responsible for overseeing security and continuity practices within their respective teams (including third parties), and facilitating compliance with security policies, processes and standards. An Enterprise Business Continuity Management (EBCM) framework has been established for Microsoft and applied to individual business units including the Cloud and Ecosystem (C&E) team under which Microsoft Azure falls. The designated C&E Business Continuity Program Office (BCPO) works with Microsoft Azure management to identify critical processes and assess risks. The C&E BCPO provides guidance to the Microsoft Azure teams on EBCM framework and BCM roadmap, which includes the following components: • Governance • Impact Tolerance; • Business Impact Analysis • Dependencies Analysis (Non-Technical and Technical) • Strategies • Planning • Testing • Training and Awareness
BCR-02: Business Continuity Management & Operational Resilience - Business Continuity Testing	*Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.*	BCPs have been documented and published for critical Azure services, which provide roles and responsibilities and detailed procedures for recovery and reconstitution of systems to a known state per defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Plans are reviewed on an annual basis, at a minimum. The BCP team conducts testing of the business continuity and disaster recovery plans for critical services, per the defined testing schedule for different loss scenarios. Each loss scenario is tested at least annually. Issues identified during testing are resolved during the exercises and plans are updated accordingly.
BCR-03: Business Continuity Management & Operational Resilience - Datacenter Utilities / Environmental Conditions	*Datacenter utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.*	Azure runs in geographically distributed Microsoft facilities, sharing space and utilities with other Microsoft Online Services. Each facility is designed to run 24x7x365 and employs various measures to help protect operations from power failure, physical intrusion, and network outages. These datacenters comply with industry standards (such as ISO/IEC 27001) for physical security and availability. They are managed, monitored, and administered by Microsoft operations personnel.
BCR-04: Business Continuity	*Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made*	Extensive documentation, including standard operating procedures, security and hardening guides, network and facility diagrams, and system build-out documentation is

Management & Operational Resilience - Documentation	*available to authorized personnel to ensure the following:* • *Configuring, installing, and operating the information system* • *Effectively using the system's security features*	maintained in a secure internal site and made available to authorized personnel. In addition, Microsoft Azure has established a C&E Security SharePoint site, assigned Privacy Leads, and designated a Security team to provide guidance on security requirements. Access to system documentation is restricted to the respective Microsoft Azure teams based on their job roles.
BCR-05: Business Continuity Management & Operational Resilience - Environmental Risks	*Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.*	Azure runs in geographically distributed Microsoft facilities, in some cases sharing space and utilities with other Microsoft Online Services (paired datacenters are located at least 300 miles apart in order to provide failover in the event of a large-scale regional disaster). Each facility is designed to run 24x7x365 and employs various measures to help protect operations from power failure, physical intrusion, and network outages. These datacenters comply with industry standards (such as ISO/IEC 27001) for physical security and availability. They are managed, monitored, and administered by Microsoft operations personnel. Microsoft Azure also provides multiple mechanisms for customers to deploy fault-tolerance within their Azure subscription environment, including the configuration of failover clusters, geo-redundant storage, and load balancing.
BCR-06: Business Continuity Management & Operational Resilience - Equipment Location	*To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.*	Microsoft datacenter site selection is performed using a number of criteria, including mitigation of environmental risks. In areas where there exists a higher probability of earthquakes, seismic bracing of the facility is employed. Environmental controls have been implemented to protect systems inside the facility, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.
BCR-07: Business Continuity Management & Operational Resilience - Equipment Maintenance	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.*	A single hardware failure is mitigated by a Fabric Controller which manages resource allocation, automatically failing-over to a different machine or cluster. Hardware management is transparent to the customer. Without additional configuration, data is protected by locally redundant storage, which maintains multiple replicas of data within a single region. If geo-replication for the virtual machine is configured, that geo-replication provides redundancy of data across regions to help ensure access to data in the event of a local disaster. Network infrastructure and components are similarly redundant, with N+1 links to regional TelCos, load balancers, and routing switch fabric.

BCR-08: Business Continuity Management & Operational Resilience - Equipment Power Failures	*Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific Business Impact Assessment*	Microsoft Azure employs sophisticated software-defined service instrumentation and monitoring that integrates at the component or server level, the datacenter edge, network backbone, Internet exchange sites, and at the real or simulated user level, providing visibility when a service disruption is occurring and pinpointing its cause. More importantly, Azure services teams continuously invest in developing greater application resiliency in software components so they will quickly recognize a disruption and gracefully fail over to a different set of servers or even a different datacenter, without interrupting the availability of the service. Azure datacenters have dedicated 24x7 uninterruptible power supply (UPS) and emergency power support, which may include generators. Regular maintenance and testing is conducted for both the UPS and generators, and datacenters have made arrangements for emergency fuel delivery. Datacenters also have a dedicated Facility Operations Center to monitor the following: Power systems, including critical electrical components – generators, transfer switch, main switchgear, power management module and uninterruptible power supply equipment.
BCR-09: Business Continuity Management & Operational Resilience - Impact Analysis	*There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following:* *• Identify critical products and services* *• Identify all dependencies, including processes, applications, business partners, and third party service providers* *• Understand threats to critical products and services* *• Determine impacts resulting from planned or unplanned disruptions and how these vary over time* *• Establish the maximum tolerable period for disruption* *• Establish priorities for recovery* *• Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption* *• Estimate the resources required for resumption*	Azure conducts a risk assessment to identify and assess continuity risks related to Microsoft Azure services. The Business Impact Analysis is carried out and impacts are assessed for critical services based on revenue and operations considerations. Business Impact Assessment, Dependency Analysis and Risk Assessments are performed /updated at least on an annual basis. Customers are responsible for performing impact analysis for their applications and design to meet their Recovery Time Objective (RTO) / Recovery Point Objective requirements.

BCR-10: Business Continuity Management & Operational Resilience - Policy	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular workforce training.*	Azure has developed a Business Continuity and Disaster Recovery (BC/DR) Standard Operating Procedure and documentation that include the defined information security and availability requirements. Microsoft Azure and/or MCIO staff are required to take training determined to be appropriate to the services being provided and the role they perform. For more information on BCDR in Azure, visit https://msdn.microsoft.com/library/azure/hh873027.aspx For general information about cloud operations and reliability in Microsoft datacenters, please visit http://www.microsoft.com/en-us/server-cloud/cloud-os/global-datacenters.aspx#Fragment_Scenario2
BCR-11: Business Continuity Management & Operational Resilience - Retention Policy	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.*	Data retention policies and procedures are defined and maintained in accordance to regulatory, statutory, contractual or business requirements. The Microsoft Azure backup and redundancy program undergoes an annual review and validation and Azure backs up infrastructure data regularly and validates restoration of data periodically for disaster recovery purposes. Customers are responsible for enforcing their own data retention policies. Microsoft Azure provides tools to securely delete data including immediately removing the index from the primary location, and removal of any geo-replicated copies of the data (index) asynchronously. Media wiping is NIST 800-88 compliant, defective disks are destroyed, and customers can only read from disk space to which they have previously written.

Change Control & Configuration Management: Controls CCC-01 through CCC-05		
CCC-01: Change Control & Configuration Management - New Development / Acquisition	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate, operations and/or datacenter facilities have been pre-authorized by the organization's business leadership or other accountable business role or function.*	Microsoft follows NIST guidance regarding security considerations in software development in that information security must be integrated into the SDLC from system inception. Continual integration of security practices in the Microsoft SDL enables early identification and mitigation of security vulnerabilities and misconfigurations; awareness of potential software coding challenges caused by required security controls; identification of shared security services and reuse of security best practices tools which improve security posture through proven methods and techniques; and enforces Microsoft's already comprehensive risk management program. Microsoft Azure has established software development and release management processes to control implementation of major changes including: • The identification and documentation of the planned change • Identification of business goals, priorities and scenarios during product planning • Specification of feature/component design • Operational readiness review based on a pre-defined criteria/check-list to assess overall risk/impact • Testing, authorization and change management based on entry/exit criteria for DEV (development), INT (Integration Testing), STAGE (Pre-production) and PROD (production) environments as appropriate. MCIO uses standardized processes for the acquisition, preparation / provisioning, deployment, and configuration of physical assets such as compute servers, storage, and networking hardware. Security processes are in place to ensure supply chain integrity, including shipping / receiving from OEM partners, physical transfers, and installations in datacenter colos. Customers are responsible for their own applications hosted in Microsoft Azure.
CCC-02: Change Control & Configuration Management - Outsourced Development	*External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g. ITIL service management processes).*	Microsoft Azure business partners and third-party contractors are required to follow the same established software development and release management processes, including SDL and OSA guidelines, to control implementation of major changes as Microsoft Azure software developers.
CCC-03: Change Control & Configuration Management - Quality Testing	*Organization shall follow a defined quality change control and testing process (e.g. ITIL Service Management) with established baselines, testing, and release standards that focus on system availability, confidentiality, and integrity of systems and services.*	Azure has developed formal standard operating procedures (SOPs) governing the change management process. These SOPs cover both software development and hardware change and release management, and are consistent with established regulatory guidelines including ISO/IEC 27001, SOC 1 / SOC 2, NIST 800-53, and others. Microsoft also uses Operational Security Assurance (OSA), a framework that incorporates the knowledge gained through a variety of capabilities that are unique to Microsoft,

		including the Microsoft Security Development Lifecycle (SDL), the Microsoft Security Response Center program, and deep awareness of the cybersecurity threat landscape. OSA combines this knowledge with the experience of running hundreds of thousands of servers in datacenters around the world. Microsoft uses OSA to minimize risk by ensuring that ongoing operational activities follow rigorous security guidelines and by validating that guidelines are actually being followed effectively. When issues arise, a feedback loop helps ensure that future revisions of OSA contain mitigations to address them. The foundation of secure online services consists of the following elements: • SDL, to ensure the software that underlies the service is designed and developed with security in mind throughout its entire lifecycle. • OSA, to ensure the deployment and operation of the service includes effective security practices throughout its lifecycle. The OSA process also uses feedback from online services teams within Microsoft to continuously evaluate and improve the OSA process. This feedback is also considered confidential, and it is protected in accordance with Microsoft internal policies. The three key processes of OSA are: • Ensuring that OSA inputs (such as organizational learning, threat intelligence, and security technologies) are up-to-date and relevant. • Developing and applying centralized review processes to consolidate requirements to establish the OSA baseline requirements. • Engaging and implementing the new requirements and baselines. Additional information on how Microsoft Azure uses OSA for change and configuration management can be found at http://www.microsoft.com/en-us/download/confirmation.aspx?id=40872.

CCC-04: Change Control & Configuration Management - Unauthorized Software Installations	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.*	Changes to production environments go through the Change Management process described in CCC-01 and CCC-03. This process also requires that: • Pre-screened admin requests from Microsoft corporate networks are approved • That role based and Just-in-Time / Just Enough Access controls are enforced • Privileges issued are temporary and grant the least privilege required to complete tasks • Multi-factor authentication for administrative access is required • Access requests are logged and audited Microsoft Azure source code libraries are limited to authorized personnel only. Where feasible, source code libraries maintain separate project work spaces for independent projects. Microsoft Azure and Microsoft Azure Contractors are granted access only to those work spaces which they need access to perform their duties. Source code libraries enforce control over changes to source code by requiring a review from designated reviewers prior to submission. An audit log detailing modifications to the source code library is maintained.
CCC-05: Change Control & Configuration Management - Production Changes	*Policies and procedures shall be established for managing the risks associated with applying changes to:* *• business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations* *• infrastructure network and systems components* *Technical measures shall be implemented to provide assurance that all changes directly correspond to a registered change request, business-critical or customer (tenant) , and/or authorization by, the customer (tenant) as per agreement (SLA) prior to deployment.*	Software releases and configuration changes to the Azure platform are tested based on established criteria prior to production implementation and procedures have been established to evaluate and implement Microsoft released patches to Azure infrastructure. Customers have access to third party audit reports and certifications that encompass the controls relevant to change management. Customers also receive their roles, rights and responsibilities in the Azure Terms & Conditions.

Data Security and Information Lifecycle Management: Controls DSI-01 through DSI-07		
DSI-01: Data Security & Information Lifecycle Management - Classification	*Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.*	Azure classifies data according to the Microsoft Azure data classification scheme and then implements a standard set of Security and Privacy attributes. Microsoft does not classify data uploaded and stored by customers. Hardware is uniquely identified using software monitoring tools and hardware asset tags as part of the Azure Data Classification program.
DSI-02: Data Security & Information Lifecycle Management - Data Inventory / Flows	*Policies and procedures shall be established to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's applications and infrastructure network and systems. In particular, providers shall ensure that data that is subject to geographic residency requirements not be migrated beyond its defined bounds.*	Internally, Microsoft tracks data flows and network connectivity among its facilities worldwide. Microsoft will not transfer Customer Data outside the geo(s) customer specifies (for example, from Europe to U.S. or from U.S. to Asia) except where necessary for Microsoft to provide customer support, troubleshoot the service, or comply with legal requirements; or where customer configures the account to enable such transfer of Customer Data, including through the use of: • Features that do not enable geo selection such as Content Delivery Network (CDN) that provides a global caching service • Web and Worker Roles, which back-up software deployment packages to the United States regardless of deployment geo • Preview, beta, or other pre-release features that may store or transfer Customer Data to the United States regardless of deployment geo • Azure Active Directory (except for Access Control), which may store Active Directory Data globally except for the United States (where Active Directory Data remains in the United States) and Europe (where Active Directory Data is in Europe and the United States) • Azure Multi-Factor Authentication, which stores authentication data in the United States.
DSI-03: Data Security & Information Lifecycle Management - e-Commerce Transactions	*Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data.*	Microsoft Azure does not provide e-commerce solutions. Note that Customer Data will be used only to provide customer the Microsoft Azure service. This may include troubleshooting aimed at preventing, detecting and repairing problems affecting the operation of the services and the improvement of features that involve the detection of, and protection against, emerging and evolving threats to the user (such as malware or spam). More information on Microsoft's commitment around use of customer data can be found in the Privacy Statement and Online Services Use Rights available at: https://azure.microsoft.com/en-us/support/legal/.
DSI-04: Data Security & Information Lifecycle Management - Handling / Labeling / Security Policy	*Policies and procedures shall be established for the labeling, handling, and security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.*	Azure has implemented a formal policy that requires assets (the definition of asset includes data and hardware) used to provide Azure services to be accounted for and have a designated asset owner. Asset owners are responsible for maintaining up-to-date information regarding their assets. The Asset Classification Standard and Asset Protection Standard describe the minimum security requirements, that employees must apply to information assets based on their

		classification. Employees, contractors and third parties responsible for managing and maintaining assets must ensure that assets are handled securely and provided with appropriate levels of protection.
DSI-05: Data Security & Information Lifecycle Management - Non-Production Data	*Production data shall not be replicated or used in non-production environments.*	The Azure platform is specifically designed and architected to prevent the possibility of production data being moved or replicated outside of the Azure cloud environment. These controls include: • Physical and logical network boundaries with strictly enforced change control policies • Segregation of duties requiring a business need to access an environment • Highly restricted physical and logical access to the cloud environment • Strict controls based on SDL and OSA that define coding practices, quality testing and code promotion • Ongoing security, privacy and secure coding practices awareness and training • Continuous logging and audit of system access • Regular compliance audits to ensure control effectiveness Microsoft Azure customers are responsible for defining policies and establishing controls for how their production data is maintained with regard to replication or high-availability and the demarcation of their production environment.
DSI-06: Data Security & Information Lifecycle Management - Ownership / Stewardship	*All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.*	Azure assets are classified in accordance with Microsoft Online Services Classification Guidelines. Azure has conducted security categorization for its information and information systems and the results are documented, reviewed and approved by the authorizing official. Asset owners are responsible for maintaining up-to-date information regarding their assets. Customers are considered the owners of their data as it exists in Azure.
DSI-07: Data Security & Information Lifecycle Management - Secure Disposal	*Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.*	Microsoft does not use customer data in non-production environments. In addition, Microsoft uses best practice procedures and a media wiping solution that is NIST 800-88 compliant. For hard drives that can't be wiped we use a destruction process that destroys it (i.e. shredding) and renders the recovery of information impossible (e.g., disintegrate, shred, pulverize, or incinerate). The appropriate means of disposal is determined by the asset type. Records of the destruction are retained. Microsoft Azure services utilize approved media storage and disposal management services. Paper documents are destroyed by approved means at the pre-determined end-of-life cycle.

Datacenter Security: Controls DCS-01 through DCS-09		
DCS-01: Datacenter Security - Asset Management	*Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership by defined roles and responsibilities.*	Microsoft Azure has implemented a formal policy that requires assets (the definition of asset includes data and hardware) used to provide Microsoft Azure services to be accounted for and have a designated asset owner. Azure asset owners are responsible for maintaining up-to-date information regarding their assets.
DCS-02: Datacenter Security - Controlled Access Points	*Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.*	Microsoft datacenters receive SSAE16/ISAE 3402 Attestation and are ISO/IEC 27001 Certified. Microsoft datacenters are located in non-descript buildings that are physically constructed, managed, and monitored 24-hours a day to protect data and services from unauthorized access as well as environmental threats. Datacenters are surrounded by a fence with access restricted through badge controlled gates. Pre-approved deliveries are received in a secure loading bay and are monitored by authorized personnel. Loading bays are physically isolated from information processing facilities. CCTV is used to monitor physical access to datacenters and the information systems. Cameras are positioned to monitor perimeter doors, facility entrances and exits, interior aisles, caged areas, high-security areas, shipping and receiving, facility external areas such as parking lots and other areas of the facilities.
DCS-03: Datacenter Security - Equipment Identification	*Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.*	MCIO, and consequently Azure, maintains a current, documented and audited inventory of equipment and network components for which it is responsible. MCIO employs automated mechanisms to detect discrepancies in device configuration by comparing them against the defined policies. MCIO turns off unused ports by default to prevent unauthorized access. Microsoft Azure Fabric Controlled Hardware Device Authentication maintains a set of credentials (keys and/or passwords) used to authenticate itself to various Microsoft Azure hardware devices under its control. The system used for transporting, persisting, and using these credentials is designed to make it unnecessary for Microsoft Azure developers, administrators, and backup services/personnel to be exposed to secret information.
DCS-04: Datacenter Security - Off-Site Authorization	*Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.*	Microsoft asset and data protection procedures provide prescriptive guidance around the protection of logical and physical data and include instructions addressing relocation. Customers control where their data is stored while using Azure services such as Site Recovery and Backup.

DCS-05: Datacenter Security - Off-Site Equipment	*Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premises. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full overwrite of the drive to ensure that the erased drive is released to inventory for reuse and deployment, or securely stored until it can be destroyed.*	Data destruction techniques vary depending on the type of data object being destroyed, whether it be subscriptions, storage, virtual machines, or databases. In Azure's multi-tenant environment, careful attention is taken to ensure that one customer's data is not allowed to either "leak" into another customer's data, or when a customer deletes data, no other customer (including, in most cases, the customer who once owned the data) can gain access to that deleted data. Azure follows NIST 800-88 Guidelines on Media Sanitization, which address the principal concern of ensuring that data is not unintentionally released. These guidelines encompass both electronic and physical sanitization.
DCS-06: Datacenter Security - Policy	*Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information.*	Microsoft Security Policy defines and establishes controls for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information. Access to media storage areas is restricted and audited. Access to Microsoft buildings is controlled, and access is restricted to those with card reader (swiping the card reader with an authorized ID badge) or biometrics for entry into Datacenters. Front desk personnel are required to positively identify Full-Time Employees (FTEs) or authorized Contractors without ID cards. Staff must wear identity badges at all times, and are required to challenge or report individuals without badges. Guests are required to wear guest badges and be escorted by authorized Microsoft personnel.
DCS-07: Datacenter Security - Secure Area Authorization	*Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.*	Datacenter entrances are guarded 24x7x365 by security personnel and access is controlled through security personnel, authorized badges, locked doors and CCTV monitoring.
DCS-08: Datacenter Security - Unauthorized Persons Entry	*Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.*	Azure Employees and contractors must have a business need to enter a Microsoft datacenter and have received prior approval. Doors between areas of differing security require authorized badge access, are monitored through logs and cameras, and audited on a regular basis. Failure to abide by the Microsoft Datacenter security policies means instant dismissal for the employee.
DCS-09: Datacenter Security - User Access	*Physical access to information assets and functions by users and support personnel shall be restricted.*	Access to Microsoft buildings is controlled, and access is restricted to those with card reader (swiping the card reader with an authorized ID badge) or biometrics for entry into Datacenters. Front desk personnel are required to positively identify Full-Time Employees (FTEs) or authorized Contractors without ID cards. Staff must wear identity badges at all times, and are required to challenge or report individuals without badges. Guests must be escorted by authorized Microsoft personnel.

Encryption and Key Management: Controls EKM-01 through EKM-04		
EKM-01: Encryption & Key Management - Entitlement	*Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.*	Microsoft has policies, procedures, and mechanisms established for effective key management to support encryption of data in storage and in transmission for the key components of the Microsoft Azure service. Microsoft provides customers the option of encrypting customer data transmitted to and from Microsoft datacenters over public networks. Microsoft uses private networks with encryption for replication of non-public customer data between Microsoft datacenters.
EKM-02: Encryption & Key Management - Key Generation	*Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.*	Microsoft has policies, procedures, and mechanisms established for effective key management to support encryption of data in storage and in transmission for the key components of the Microsoft Azure service. Microsoft provides customers the option of encrypting customer data transmitted to and from Microsoft datacenters over public networks. Microsoft uses private networks with encryption for replication of non-public customer data between Microsoft datacenters. The certificates, keys and other credentials used for internal communication among Microsoft Azure components such as Fabric Controller (FC), Fabric Agent (FA), and Management Portal are stored in the Microsoft Azure secret store for use in deployment. The Secret Store Service stores and manages credentials used by Microsoft Azure platform components. See also the response to EKM-04.
EKM-03: Encryption & Key Management - Sensitive Data Protection	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.*	The following are some capabilities of Secret Store (noted in the response to EKM-02) that are relevant to cryptographic key management: Security: • Access to Secret Store is over an encrypted channel • Cryptographic key information is stored in an encrypted form • Tamper resistant auditing of access to the secret store Automated Key Management: • Automatic generation of key pairs and certificates • Automatic and secure storage of the key pair information in a database • Automatic on-demand, minimal downtime key rollovers Alerting and Reporting: • Alerting on certificates that will expire in next N days.

EKM-04: Encryption & Key Management - Storage and Access	*Platform and data-appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.*	Key management encompasses the entire life cycle of cryptographic keys. A key has three phases during its life, namely - Pre-Operational, Operational and Post-Operational. Azure Crypto algorithms / Key lengths: • Symmetric Block: AES >=256 bit • Block Cipher Modes: CBC, CCM, GCM • Asymmetric: RSA (>=2048bit), Diffie-Hellman (>= 2048bit), ECC (>= 256bit), Elliptic Curve Cryptography P-256 or greater • Hash (including HMAC usage): SHA-2 (SHA-256, SHA-384, SHA-512) • HMAC Key Lengths: >=128 bit

Governance and Risk Management: Controls GRM-01 through GRM-11		
GRM-01: Governance and Risk Management - Baseline Requirements	*Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and authorized based on business need.*	As part of the overall ISMS framework, baseline security requirements (such as for Operating System deployments) are constantly being reviewed, improved and implemented. In addition, MCIO-managed network devices are configured to log and collect security events, and monitored for compliance with established security standards. Prior to any deployment, a change to the baseline must follow and adhere to the change and release management process. Tickets are opened to track any configuration or configuration deployment changes. Tickets are also opened for any baseline settings/rules changes before being deployed.
GRM-02: Governance and Risk Management - Data Focus Risk Assessments	*Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following:* • *Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure* • *Compliance with defined retention periods and end-of-life disposal requirements* • *Data classification and protection from unauthorized use, access, loss, destruction, and falsification*	Microsoft Azure Management requires personnel to adhere to Microsoft Cloud Services' Microsoft Security Policy and applicable standards, and to follow approved procedures. In order to meet Microsoft Azure policies and objectives, Microsoft Azure will coordinate with other security organizations, property security groups and corporate functions such as Facilities, Human Resources (HR), Information Technology, Internal Audit, Legal and Corporate Affairs (LCA), Sales and Marketing, and Trustworthy Computing (TwC) within Microsoft. This risk assessment was developed as part of the ISO/IEC 27001 in accordance with NIST 800-30 standard. In order to facilitate the risk assessment process, the following general steps were considered: • Determine the extent of potential threat • Identify which security controls in a system need to be applied • Summarize residual risk • Involve senior management to address specific actions taken or planned to correct deficiencies in security controls • Reduce or eliminate known vulnerabilities in the information system. Vulnerabilities identified for the risk assessment were based on available NIST 800-30, NIST 800-53, and National Vulnerability database (U.S. government repository of standards-based vulnerability management data) guidance. The risk assessment includes data collected in interviews, input from the compliance v-team and reviews of system and design documents. The level of risk was assessed by evaluating collected risk-related attributes regarding threats, vulnerabilities, assets and resources, current controls, and the associated likelihood that vulnerability could be exploited by a potential threat and the impact (e.g., magnitude of loss resulting from such exploitation).

GRM-03: Governance and Risk Management - Management Oversight	*Managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to their area of responsibility.*	Microsoft staff take part in a Microsoft Azure and/or MCIO-sponsored security training program, and are recipients of periodic security awareness updates when applicable. Security education is an on-going process and is conducted regularly in order to minimize risks. An example of an internal training is Microsoft Security 101. Microsoft also has non-disclosure provisions in our employee contracts. Microsoft Azure and/or MCIO staff are required to take training determined to be appropriate to the services being provided and the role they perform.
GRM-04: Governance and Risk Management - Management Program	*An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business:* • *Risk management* • *Security policy* • *Organization of information security* • *Asset management* • *Human resources security* • *Physical and environmental security* • *Communications and operations management* • *Access control* • *Information systems acquisition, development, and maintenance*	An ISMP has been established to enable Microsoft Azure to maintain and improve its management system for information security. Through establishment of the ISMS, Azure plans for and manages protection of its assets to acceptable security levels based on defined risk management processes. In addition, Azure monitors the ISMS and the effectiveness of controls in maintaining the confidentiality, integrity and availability of assets to continuously improve information security. The ISMS framework encompasses industry best-practices for information security and privacy. The ISMS has been documented and communicated in a customer-facing Microsoft Security Policy, which can be made available upon request (customers and prospective customers must have a signed NDA or equivalent in place to receive a copy). Microsoft Azure performs annual ISMS reviews, the results of which are reviewed by management. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.
GRM-05: Governance and Risk Management - Management Support / Involvement	*Executive and line management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has been assigned.*	Microsoft Azure has designed and implemented an ISMS framework that addresses industry best-practices for information security and privacy. The ISMS has been documented and communicated in a customer-facing Microsoft Security Policy, which can be made available upon request (customers and prospective customers must have a signed NDA or equivalent in place to receive a copy). This policy is reviewed and approved annually by Microsoft Azure management, who has established roles and responsibilities to oversee implementation of the policy. Each management-endorsed version of the Microsoft Security Policy and subsequent updates are distributed to relevant stakeholders. The Microsoft Security Policy is made available to new and existing Microsoft Azure employees for review as part of an information security education and awareness program. Azure employees represent that they have reviewed, and agree to adhere to, all policies within the Microsoft Security Policy documents. Microsoft Azure Contractor Staff agree to adhere to the relevant policies within the Microsoft Security Policy.

GRM-06: Governance and Risk Management - Policy	*Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.*	A customer facing version of the Microsoft Security Policy can be made available upon request. Customers and prospective customers must have a signed NDA or equivalent in order to receive a copy of the Microsoft Security Policy. The Microsoft Security Policy is made available to new and existing Microsoft Azure employees for review as part of an information security education and awareness program. Microsoft Azure employees represent that they have reviewed, and agree to adhere to, all policies within the Microsoft Security Policy documents. Microsoft Azure Contractor Staff agree to adhere to the relevant policies within the Microsoft Security Policy.
GRM-07: Governance and Risk Management - Policy Enforcement	*A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures.*	Azure services staff suspected of committing breaches of security and/or violating the Microsoft Security Policy equivalent to a Microsoft Code of Conduct violation are subject to an investigation process and appropriate disciplinary action up to and including termination. Contracting staff suspected of committing breaches of security and/or violations of the Microsoft Security Policy are subject to formal investigation and action appropriate to the associated contract, which may include termination of such contracts. Human Resources is responsible for coordinating disciplinary response.
GRM-08: Governance and Risk Management - Policy Impact on Risk Assessments	*Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.*	Microsoft Azure performs risk assessments of its environment to review the effectiveness of information security controls and safeguards, as well as to identify new risks. The risks are assessed annually and the results of the risk assessment are presented to management through a formal risk assessment report.
GRM-09: Governance and Risk Management - Policy Reviews	*The organization's business leadership (or other accountable business role or function) shall review the Microsoft Security Policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.*	The Microsoft Security Policy undergoes a formal management review and update process at a regularly scheduled interval not to exceed 1 year. In the event a significant change is required in the security requirements, it may be reviewed and updated outside of the regular schedule.

GRM-10: Governance and Risk Management - Risk Assessments	*Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).*	Azure performs an annual risk assessment. As part of the overall ISMS framework, baseline security requirements are constantly being reviewed, improved and implemented. Azure's controls for risk and vulnerability assessment of the Azure infrastructure encompass all areas in this section and meet the requirements of the standards against which we audit, as demonstrated by reports identified on the Azure Trust Center website.
GRM-11: Governance and Risk Management - Risk Management Framework	*Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and stakeholder approval.*	Azure has established a risk management framework, and related processes, for assessing the applicable IT risks and performs an annual risk assessment that covers security, continuity, and operational risks. As part of this process, threats to security are identified and the risk from these threats is formally assessed. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.

Human Resources: Controls HRS-01 through HRS-11		
HRS-01: Human Resources - Asset Returns	*Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period.*	Employees, contractors and third party users are formally notified to destroy or return, as applicable, any physical materials that Microsoft has provided to them during the term of employment or the period of Contractor agreement and any electronic media must be removed from Contractor or third party infrastructure. Microsoft may also conduct an audit to make sure data is removed in an appropriate manner.
HRS-02: Human Resources - Background Screening	*Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.*	Pursuant to local laws, regulations, ethics and contractual constraints, Microsoft US-based full-time employees (FTE) are required to successfully complete a standard background check as part of the hiring process. Background checks may include but are not limited to review of information relating to a candidate's education, employment, and criminal history. Third-party contractors are subject to the hiring practices of their organizations, and contractor agencies must adhere to equivalent standards exercised by Microsoft.
HRS-03: Human Resources - Employment Agreements	*Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.*	Microsoft Azure contractor staff and FTE staff are required to take any training determined to be appropriate to the services being provided and the role they perform.
HRS-04: Human Resources - Employment Termination	*Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.*	Microsoft Corporate Human Resources Policy drives employee termination processes and Microsoft Policy clearly defines roles and responsibilities. Termination policies and procedures cover all aspects of separation including return of assets, badges, computer equipment and data. Human Resources also manages revocation of access to resources, both physical and electronic.
HRS-05: Human Resources - Mobile Device Management	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring).*	Microsoft Azure teams and personnel are required to adhere to applicable policies, which do not permit mobile computing devices to be connected to the production environment. Mobile computing access points on Microsoft's corporate network are required to adhere to wireless device security requirements.
HRS-06: Human Resources - Non-Disclosure Agreements	*Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals.*	Microsoft Legal and Human Resources maintain policies and procedures defining the implementation and execution of non-disclosure and confidentiality agreements.

HRS-07: Human Resources - Roles / Responsibilities	*Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.*	The Microsoft Security Policy exists in order to provide Microsoft Azure Staff and Contractor Staff with a current set of clear and concise Information Security Policies including their roles and responsibilities related to information assets and security. These policies provide direction for the appropriate protection of Microsoft Azure. The Microsoft Security Policy has been created as a component of an overall Information Security Management System (ISMS) for Microsoft Azure. The Policy has been reviewed, approved, and is endorsed by Microsoft Azure management.
HRS-08: Human Resources - Technology Acceptable Use	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to corporate resources (i.e., BYOD) shall be considered and incorporated as appropriate.*	Mobile / wireless devices are not permitted within Microsoft datacenters where customer data is stored. Wireless access to Azure production and/or customer environments is prohibited.
HRS-09: Human Resources - Training / Awareness	*A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.*	Microsoft staff take part in a Microsoft Azure and/or MCIO-sponsored security training program, and are recipients of periodic security awareness updates when applicable. Security education is an ongoing process and is conducted regularly in order to minimize risks. An example of an internal training is Microsoft Security 101. Microsoft also has non-disclosure provisions in employee contracts.
HRS-10: Human Resources - User Responsibility	*All personnel shall be made aware of their roles and responsibilities for:* • *Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations* • *Maintaining a safe and secure working environment*	Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire and annually thereafter. In addition, employees must acknowledge Microsoft's Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage, on an annual basis.
HRS-11: Human Resources - Workspace	*Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions are disabled after an established period of inactivity.*	MCIO inherits the Microsoft corporate AD session lock functionality and enforces session lock outs after a defined period of inactivity. Terminal Server boundary protection devices limit the number of sessions that can be established to an MCIO host to one. Network connections are terminated after a defined period of inactivity.

Identity and Access Management: Controls IAM-01 through IAM-13		
IAM-01: Identity & Access Management - Audit Tools Access	*Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.*	Log and monitor access is highly restricted to only authorized staff with a business need to access such systems. Microsoft Azure platform components (including OS, Virtual Network, Fabric, etc.) are configured to log and collect security events.
IAM-02: Identity & Access Management - Credential Lifecycle / Provision Management	*User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following:* • *Procedures and supporting roles and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships)* • *Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems)* • *Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant))* • *Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation)* • *Account credential lifecycle management from instantiation through revocation* • *Account credential and/or identity store minimization or re-use when feasible*	Microsoft Azure has adopted applicable corporate and organizational security policies, including an Microsoft Security Policy. The policies have been approved, published and communicated across Azure teams. The Microsoft Security Policy requires that access to Microsoft Azure assets to be granted based on business justification, with the asset owner's authorization and limits based on "need-to-know" and "least-privilege" principles. In addition, the policy also addresses requirements for access management lifecycle including access provisioning, authentication, access authorization, removal of access rights and periodic access reviews. Access to Microsoft buildings is controlled, and access is restricted to those with card reader (swiping the card reader with an authorized ID badge) or biometrics for entry into Datacenters. Front desk personnel are required to positively identify Full-Time Employees (FTEs) or authorized Contractors without ID cards. Staff must wear identity badges at all times, and are required to challenge or report individuals without badges. Guests must be escorted by authorized Microsoft personnel. Password policies for corporate domain accounts are managed through Microsoft corporate Active Directory policy that specifies minimum requirements for password length, complexity and expiry. Temporary passwords are communicated to users using Microsoft's established processes. Azure services and infrastructure must at a minimum meet Microsoft corporate requirements, but an internal organization can increase the strength beyond this standard, on their own discretion and to meet their security needs. Microsoft Azure uses Active Directory (AD) to manage user accounts. Security group membership must be approved by the designated security group owners within Microsoft Azure. Automated procedures are in place to disable AD accounts upon the user's leave date. Domain-level user accounts are disabled after 90 days of inactivity.

	• *Authentication, authorization, and accounting (AAA) rules for access to data and sessions (e.g., encryption and strong/multi-factor, expireable, non-shared authentication secrets)* • *Permissions and supporting capabilities for customer (tenant) controls over authentication, authorization, and accounting (AAA) rules for access to data and sessions* • *Adherence to applicable legal, statutory, or regulatory compliance requirements*	
IAM-03: Identity & Access Management - Diagnostic / Configuration Ports Access	*User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.*	Access control policy is a component of overall policies and undergoes a formal review and update process. Access to Microsoft Azure s' assets is granted based upon business requirements and with the asset owner's authorization. Additionally: • Access to assets is granted based upon need-to-know and least-privilege principles • Where feasible, role-based access controls are used to allocate logical access to a specific job function or area of responsibility, rather than to an individual • Physical and logical access control policies are consistent with standards Microsoft Azure controls physical access to diagnostic and configuration ports through physical datacenter controls. Diagnostic and configuration ports are only accessible by arrangement between service/asset owner and hardware/software support personnel requiring access. Ports, services, and similar facilities installed on a computer or network facility, which are not specifically required for business functionality, are disabled or removed.
IAM-04: Identity & Access Management - Policies and Procedures	*Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.*	Microsoft Azure uses Active Directory (AD) to manage user accounts. Security group membership must be approved by the designated security group owners within Microsoft Azure. Automated procedures are in place to disable AD accounts upon the user's leave date. Domain-level user accounts are disabled after 90 days of inactivity. MCIO enforces segregation of duties through user defined groups to minimize the risk of unintentional or unauthorized access or change to production systems. Information system access is restricted based on the user's job responsibilities. Documentation on how Microsoft Azure maintains segregation of duties is included in the available security framework audit results on the Azure Trust Center website.
IAM-05: Identity & Access Management - Segregation of Duties	*User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.*	Segregation of duties is established on critical functions within the Microsoft Azure environment to minimize the risk of unintentional or unauthorized access or change to production systems. Duties and responsibilities are segregated and defined between Microsoft Azure operations teams. Asset owners/custodians approve different access levels and privileges in the production environment.

		Segregation of duties is implemented in Microsoft Azure s' environments in order to minimize the potential of fraud, misuse, or error.
IAM-06: Identity & Access Management - Source Code Access Restriction	*Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.*	Access to Azure source code libraries is limited to authorized personnel. Where feasible, source code libraries maintain separate project work spaces for independent projects. Microsoft Azure and Contractors are granted access only to those work spaces to which they need access to perform their duties. Source code libraries enforce control over changes to source code by requiring a review from designated managers prior to submission. An audit log detailing modifications to the source code library is maintained.
IAM-07: Identity & Access Management - Third Party Access	*The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.*	Identification, assessment, and prioritization of risks related to external parties and access controls is performed as part of Azure's risk management program and verified as part of the ISO/IEC 27001 audit. Third party security and privacy requirements are established through vendor due-diligence reviews, conducted by the designated Microsoft Azure manager, and included in signed contractual agreements prior to engaging in third party services. The engaging team within Azure is responsible for managing their third party relationships, including contract management, monitoring of metrics such as service level agreements, and vendor access to relevant applications.
IAM-08: Identity & Access Management - Trusted Sources	*Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.*	Microsoft Azure uses Active Directory (AD) to manage user accounts. Security group membership must be approved by the designated security group owners within Microsoft Azure. Automated procedures are in place to disable AD accounts upon the user's leave date. Domain-level user accounts are disabled after 90 days of inactivity. MCIO enforces segregation of duties through user defined groups to minimize the risk of unintentional or unauthorized access or change to production systems. Information system access is restricted based on the user's job responsibilities. Documentation on how Microsoft Azure maintains segregation of duties is included in the available security framework audit results on the Azure Trust Center website.
IAM-09: Identity & Access Management - User Access Authorization	*Provisioning user access (e.g., employees, contractors, customers (tenants), business partners and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, provider shall inform customer (tenant) of this user access, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.*	Microsoft Azure uses Active Directory (AD) to manage and provision user accounts. Security group membership must be approved by the designated security group owners within Microsoft Azure. Automated procedures are in place to disable AD accounts upon the user's leave date. Domain-level user accounts are disabled after 90 days of inactivity. Strong authentication, including the use of multi-factor authentication, helps limit access to customer data to authorized personnel only. Sample audits are performed by both Microsoft and third parties to attest that access is only for appropriate business purposes. When access is granted, it is carefully controlled and logged, and revoked as soon as it is no longer needed. The operational processes and controls that govern access and use of customer data in Azure are rigorously maintained and regularly verified by accredited audit firms.

IAM-10: Identity & Access Management - User Access Reviews	*User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow established user access policies and procedures.*	Microsoft's Security Policy requires that access to Azure assets be granted based on business justification, with the asset owner's authorization and limited based on "need-to-know" and "least-privilege" principles. In addition, the policy also addresses requirements for access management lifecycle including access provisioning, authentication, access authorization, removal of access rights and periodic access reviews. Managers and owners of applications and data are responsible for reviewing who has access on a periodic basis. Customers control access by their own users and are responsible for ensuring appropriate review of such access.
IAM-11: Identity & Access Management - User Access Revocation	*Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.*	Designated security group owners within Microsoft Azure are responsible for reviewing appropriateness of employee access to applications and data on a periodic basis. Regular access review audits occur to validate appropriate access provisioning has taken place. Access is modified based on the results of this review. Membership in security groups must be approved by security group owners. Automated procedures are in place to disable AD accounts upon the user's leave-date. Physical access to infrastructure systems is restricted to Microsoft operations personnel or designated and authorized third-party contractors at datacenter locations. Access is logged and reviewed by security managers. Within the Microsoft Azure environment, customers are responsible for managing access to the applications customers host on Microsoft Azure.
IAM-12: Identity & Access Management - User ID Credentials	*Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures:* • *Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation)* • *Account credential lifecycle management from instantiation through revocation* • *Account credential and/or identity store minimization or re-use when feasible* • *Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong / multi-factor, expireable, non-shared authentication secrets)*	Password policies for corporate domain accounts are managed through Microsoft corporate Active Directory policy that specifies minimum requirements for password length, complexity and expiry. Temporary passwords are communicated to users using Microsoft's established processes. Azure services and infrastructure must at a minimum meet Microsoft internal IT requirements, but an internal organization can increase the strength past this standard, on their own discretion and to meet their security needs. Customers are responsible for keeping passwords from being disclosed to unauthorized parties and for choosing passwords with sufficient entropy as to be effectively non-guessable and for deployment of services such as multi-factor authentication.

IAM-13: Identity & Access Management - Utility Programs Access	*Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.*	Administrative access and privileges to the Azure infrastructure or platform are restricted to authorized personnel through designated AD security groups based on job responsibilities. Security group membership must be approved by the designated security group owners within Microsoft Azure. Utility programs undergo changes through the release management process and are restricted to authorized personnel only.

Infrastructure and Virtualization Security: Controls IVS-01 through IVS-13		
IVS-01: Infrastructure & Virtualization Security - Audit Logging / Intrusion Detection	*Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.*	Logging of service, user and security events (web server logs, FTP server logs, etc.) is enabled and retained centrally. MCIO restricts access to audit logs to authorized personnel based on job responsibilities. Event logs are archived on secure infrastructure and are retained for 180 days. Microsoft Identity Manager and intrusion detection system tools are implemented within the Azure environment. Azure uses an early warning system to support real-time analysis of security events within its operational environment. Monitoring agents and the alert and incident management system generate near real-time alerts about events that could potentially compromise the system.
IVS-02: Infrastructure & Virtualization Security - Change Detection	*The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g. dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g. portals or alerts).*	Each OS (Host OS, Guest OS, Native OS) is deployed via a "Base Image". The base image is constructed through a formal build process. Each base image is built upon an OS version in which the kernel, and many other core components, have been modified and optimized to support the Azure environment. Host OS and Native OS are hardened operating system images that run on compute (runs as first VM on the node) & storage nodes, and host the fabric agent. This has the benefit of reducing the surface area exposed by APIs or unused components. This reduced-footprint operating system includes only those components necessary to the Azure environment, which both improves performance and reduces the potential attack surface. The baseline configuration lifecycle defines a repeatable process by which baselines are established, evolved and monitored. Five distinct stages create a framework for managing the lifecycle of a baseline: establish and update, implementation (adoption and deployment), scan, reporting, review and analysis. These processes also apply to Web and Worker roles in Azure Cloud Services, as well as OS gallery images. Customers are responsible for managing virtual machines running as IaaS within their tenant environment.
IVS-03: Infrastructure & Virtualization Security - Clock Synchronization	*A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.*	MCIO has established procedures to synchronize servers and network devices in the Azure environment with NTP Stratum 1 time servers that sync off of the Global Positioning System (GPS) satellites. The synchronization is performed automatically every five minutes.

IVS-04: Infrastructure & Virtualization Security - Information System Documentation	*The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.*	The following operational processes are in place: • Proactive capacity management based on defined thresholds or events • Hardware and software subsystem monitoring for acceptable service performance and availability, service utilization, storage utilization and network latency Customers are responsible for monitoring and planning the capacity needs of their applications and tenant environment. Proactive monitoring continuously measures the performance of key subsystems of the Azure services platform against the established boundaries for acceptable service performance and availability. When a threshold is reached or an irregular event occurs, the monitoring system generates warnings so that operations staff can address the threshold or event.
IVS-05: Infrastructure & Virtualization Security - Vulnerability Management	*Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g. virtualization aware).*	Procedures have been established and implemented to regularly scan for vulnerabilities on hypervisor hosts. Vulnerability scanning is performed on server operating systems, databases, and network devices with the appropriate vulnerability scanning tools. The vulnerability scans are performed on a quarterly basis at a minimum. Azure contracts with independent assessors to perform penetration testing of the Azure boundary. Red-Team / Blue-Team exercises are also routinely performed and results used to make security improvements.
IVS-06: Infrastructure & Virtualization Security - Network Security	*Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, and ports, and by compensating controls.*	Firewall rules and ACLs are documented and reviewed on at least a quarterly basis. Changes are required to follow the approved firewall rule change control process. Traffic flow policies are implemented on boundary protection devices that deny traffic by default. These policies are reviewed every month to determine any changes required.
IVS-07: Infrastructure & Virtualization Security - OS Hardening and Base Controls	*Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.*	Public consensus-based industry best practices are utilized to define an initial baseline. The Azure team leverages industry-standard security benchmarks to assist in the establishment of initial baselines, after which product and technical subject matter experts review the benchmarks and where appropriate customize the base settings further. This customization may include the addition or removal of rules or rule updates. Upon completion of this review and customization, the initial baseline is presented for approval. Once approved, the initial baseline is established. It is a customer responsibility to harden any VM operating systems or templates. Microsoft Azure software and hardware configurations are reviewed at least quarterly to identify and eliminate any unnecessary functions, ports, protocols and services.
IVS-08: Infrastructure & Virtualization Security - Production /	*Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm*	For the Azure infrastructure, production and non-production environments are physically and logically separated. Microsoft Azure employs network-based and host-based boundary protection devices such as firewalls, load balancers, IP Filters, and front-end components. These devices use mechanisms such as VLAN isolation, NAT and

Non-Production Environments	*authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.*	packet filtering to separate customer traffic from management traffic. Azure provides guidance on configuring multiple environments through web documentation, blogs, TechNet, diagrams, Video on Demand and through Azure web-based training. Within the Azure platform, tenants define their own production and non-production environments.
IVS-09: Infrastructure & Virtualization Security - Segmentation	*Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations:* • *Established policies and procedures* • *Isolation of business critical assets and/or sensitive user data, and sessions that mandate stronger internal controls and high levels of assurance* • *Compliance with legal, statutory and regulatory compliance obligations*	Azure employs a defense in depth strategy for boundary protection, including secure segmentation of network environments through several methods including VLANs, ACL restrictions and encrypted communications for remote connectivity.
IVS-10: Infrastructure & Virtualization Security - VM Security	*Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from production-level networks for such migrations.*	Communication channels are logically or physically isolated from other networks. Customer information is encrypted during transmission over external networks. Customer configuration information (e.g. connection strings, application settings) supplied through the management portal is protected while in transit and at rest.
IVS-11: Infrastructure & Virtualization Security - Hypervisor Hardening	*Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).*	Microsoft Azure enforces the concept of least privilege and restricts access to information systems including the hypervisor or hypervisor management plane using role based security groups.
IVS-12: Infrastructure & Virtualization Security - Wireless Security	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following:* • *Perimeter firewalls implemented and configured to restrict unauthorized traffic* • *Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings)*	Azure does not permit or allow wireless connections in the Azure network environment. Azure regularly scans for rogue wireless signals on a quarterly basis and rogue signals are investigated and removed.

	• *User access to wireless network devices restricted to authorized personnel* • *The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network*	
IVS-13: Infrastructure & Virtualization Security - Network Architecture	*Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.*	Internal Azure diagrams clearly define boundaries and data flows between zones having different data classification, trust levels or compliance and regulatory requirements. Communication channels are logically or physically isolated from other networks. Customer information is encrypted during transmission over external networks. Customer configuration information (e.g. connection strings, application settings) supplied through the management portal is protected while in transit and at rest. Network filtering is implemented to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted platform components. The Microsoft Azure network is segregated to separate customer traffic from management traffic. In addition, the SQL Azure services layer includes TDS gateways that control information flows through stateful inspection. Microsoft Azure has implemented load balancers and traffic filters to control the flow of external traffic to Microsoft Azure components. Additionally, Microsoft Azure has established automated controls to monitor and detect internally initiated Denial of Service attacks.

Interoperability and Portability: Controls IPY-01 through IPY-05		
IPY-01: Interoperability & Portability - APIs	*The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.*	A full set of Windows PowerShell cmdlets for the Azure API Management API is available via the standard Azure PowerShell installer. For more information, see https://azure.microsoft.com/en-us/services/api-management/
IPY-02: Interoperability & Portability - Data Request	*All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files)*	Azure customers own their data—that is, all data, including text, sound, video, or image files and software, that are provided to Microsoft by or on the customer's behalf, through use of Azure. Customers can access their data at any time and for any reason without assistance from Microsoft. Microsoft will use customer data only to provide the services agreed upon, including purposes that are compatible with providing those services. Azure provides authenticated and logged access to customer data which restricts access to it by Microsoft personnel and subcontractors. We also take strong steps to protect your customer data from inappropriate use or loss, and to segregate customer data on shared hardware from that of other customers.
IPY-03: Interoperability & Portability - Policy & Legal	*Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence.*	Azure policies and provisions provide for language agnostic Microsoft Azure Storage Services REST APIs, Microsoft Azure Service Management REST APIs, AppFabric Service Bus REST APIs, AppFabric Access Control REST APIs using open, standard formats such as HTTP, XML, WRAP, and SWT along with an ecosystem of tools and libraries,
IPY-04: Interoperability & Portability - Standardized Network Protocols	*The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.*	Access to customer applications and data through the service management API requires authentication using the customer registered certificate over SSL. Access to a Storage Account is restricted through the designated Storage Account Key (SAK) or customer generated Shared Access Signature (SAS). Access to media assets and content keys through the REST API requires authentication over SSL. Customer media assets are stored in customer specified storage accounts. Content keys and customer storage account credentials (i.e., SAK and SAS) are encrypted while at rest. Customer media is stored securely during content transformation and deleted upon completion of the requested transformation. Delivery of a media asset is based on customer defined access policy.
IPY-05: Interoperability & Portability - Virtualization	*The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use and all solution-specific virtualization hooks available for customer review.*	Microsoft Azure supports industry standards; please visit https://msdn.microsoft.com/en-us/library/azure/dn495227.aspx for additional information.

Mobile Security: Controls MOS-01 through MOS-20		
MOS-01: Mobile Security - Anti-Malware	*Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.*	Mobile / wireless devices are not permitted within Microsoft datacenters where customer data is stored. Wireless access to Azure production and/or customer environments is prohibited.
MOS-02: Mobile Security - Application Stores	*A documented list of approved application stores has been defined as acceptable for mobile devices accessing or storing provider managed data.*	See response to MOS-01.
MOS-03: Mobile Security - Approved Applications	*The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.*	See response to MOS-01.
MOS-04: Mobile Security - Approved Software for BYOD	*The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage.*	See response to MOS-01.
MOS-05: Mobile Security - Awareness and Training	*The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and training program.*	See response to MOS-01.
MOS-06: Mobile Security - Cloud Based Services	*All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.*	See response to MOS-01.
MOS-07: Mobile Security - Compatibility	*The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.*	See response to MOS-01.
MOS-08: Mobile Security - Device Eligibility	*The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.*	See response to MOS-01.
MOS-09: Mobile Security - Device Inventory	*An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD)) will be included for each device in the inventory.*	See response to MOS-01.
MOS-10: Mobile Security - Device Management	*A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.*	See response to MOS-01.

MOS-11: Mobile Security - Encryption	*The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and shall be enforced through technology controls.*	See response to MOS-01.
MOS-12: Mobile Security - Jailbreaking and Rooting	*The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g. jailbreaking or rooting) and shall enforce the prohibition through detective and preventative controls on the device or through a centralized device management system (e.g. mobile device management).*	See response to MOS-01.
MOS-13: Mobile Security - Legal	*The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the expectations regarding the loss of non-company data in the case a wipe of the device is required.*	See response to MOS-01.
MOS-14: Mobile Security - Lockout Screen	*BYOD and/or company-owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.*	See response to MOS-01.
MOS-15: Mobile Security - Operating Systems	*Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.*	See response to MOS-01.
MOS-16: Mobile Security - Passwords	*Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.*	See response to MOS-01.
MOS-17: Mobile Security - Policy	*The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).*	See response to MOS-01.
MOS-18: Mobile Security - Remote Wipe	*All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT.*	See response to MOS-01.
MOS-19: Mobile Security - Security Patches	*Mobile devices connecting to corporate networks, or storing and accessing company information, shall allow for remote software version/patch validation. All mobile devices shall have the latest available security-related*	See response to MOS-01.

	patches installed upon general release by the device manufacturer or carrier and authorized IT personnel shall be able to perform these updates remotely.	
MOS-20: Mobile Security - Users	*The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.*	See response to MOS-01.

Security Incident Management, E-Discovery & Cloud Forensics: Controls SEF-01 through SEF-05		
SEF-01: Security Incident Management, E-Discovery & Cloud Forensics - Contact / Authority Maintenance	*Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.*	Microsoft Azure has designated responsibilities and established processes to maintain contacts with external authorities across the jurisdictions in which it operates.
SEF-02: Security Incident Management, E-Discovery & Cloud Forensics - Incident Management	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.*	Microsoft Azure has developed robust processes to facilitate a coordinated response to incidents if one was to occur. A security event may include, among other things, unauthorized access resulting in loss, disclosure or alteration of data. The Azure Incident Response process follows five main phases: • Identification – System and security alerts may be harvested, correlated, and analyzed. Events are investigated by Microsoft operational and security organizations. If an event indicates a security issue, the incident is assigned a severity classification and appropriately escalated within Microsoft. This escalation will include product, security, and engineering specialists. • Containment – The escalation team evaluates the scope and impact of an incident. The immediate priority of the escalation team is to ensure the incident is contained and data is safe. The escalation team forms the response, performs appropriate testing, and implements changes. In the case where in-depth investigation is required, content is collected from the subject systems using best-of-breed forensic software and industry best practices. • Eradication – After the situation is contained, the escalation team moves toward eradicating any damage caused by the security breach, and identifies the root cause for why the security issue occurred. If a vulnerability is determined, the escalation team reports the issue to product engineering. • Recovery – During recovery, software or configuration updates are applied to the system and services are returned to a full working capacity. • Lessons Learned – Each security incident is analyzed to ensure the appropriate mitigations applied to protect against future reoccurrence.
SEF-03: Security Incident Management, E-Discovery & Cloud Forensics	*Workforce personnel and external business relationships shall be informed of their responsibilities and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security*	MCIO has established procedures to receive, generate and disseminate security alerts from external organizations as necessary. MCIO coordinates with external agencies regarding the implementing of security directives. The Azure logging and monitoring infrastructure

- Incident Reporting	*events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.*	encompasses the entire Azure platform and does not vary by tenant. Detected incidents are isolated or contained in the most effective way depending on the nature of the event.
SEF-04: Security Incident Management, E-Discovery & Cloud Forensics - Incident Response Legal Preparation	*Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.*	In the event a follow-up action concerning a person or organization after an information security incident requires legal action, proper forensic procedures including chain of custody shall be required for preservation and presentation of evidence to support potential legal action subject to the relevant jurisdiction. Upon notification, impacted customers (tenants) and/or other external business relationships of a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation. Security incident response plans and collection of evidence adheres to ISO/IEC 27001 standards. MCIO has established processes for evidence collection and preservation for troubleshooting an incident and analyzing the root cause. In case a security incident involves legal action such as subpoena form, the guidelines described in the TSG are followed.
SEF-05: Security Incident Management, E-Discovery & Cloud Forensics - Incident Response Metrics	*Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.*	An incident management framework has been established and communicated with defined processes, roles and responsibilities for the detection, escalation and response of incidents. Incident management teams perform 24x7 monitoring, including documentation, classification, escalation and coordination of incidents per documented procedures. Events, thresholds and metrics have been defined and configured to detect incidents and alert the appropriate Azure teams.

Supply Chain Management, Transparency and Accountability: Controls STA-01 through STA-09		
STA-01: Supply Chain Management, Transparency and Accountability - Data Quality and Integrity	*Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.*	Third party vendors are required to comply with Microsoft security policies and are audited. The Hardware Supply Management (HSM) group works with the MCIO business groups to protect against supply chain threats throughout the supply chain lifecycle. HSM supports MCIO in creating purchase orders, accelerating deliveries, performing quality checks, processing warranty claims and obtaining spares.
STA-02: Supply Chain Management, Transparency and Accountability - Incident Reporting	*The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g. portals).*	Azure maintains and notifies customers of potential changes and events that may impact security or availability of the services through an online Service Dashboard. Changes to the security commitments and security obligations of Microsoft Azure customers are updated on the Microsoft Azure website in a timely manner.
STA-03: Supply Chain Management, Transparency and Accountability - Network / Infrastructure Services	*Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.*	Microsoft Azure employs sophisticated software-defined service instrumentation and monitoring that integrates at the component or server level, the datacenter edge, our network backbone, Internet exchange sites, and at the real or simulated user level, providing visibility when a service disruption is occurring and pinpointing its cause. Proactive monitoring continuously measures the performance of key subsystems of the Microsoft Azure services platform against the established boundaries for acceptable service performance and availability. When a threshold is reached or an irregular event occurs, the monitoring system generates warnings so that operations staff can address the threshold or event.
STA-04: Supply Chain Management, Transparency and Accountability - Provider Internal Assessments	*The provider shall perform annual internal assessments of conformance to, and effectiveness of, its policies, procedures, and supporting measures and metrics.*	Microsoft Azure performs risk assessments of its environment to review the effectiveness of information security controls and safeguards, as well as to identify new risks. The risks are assessed annually and the results of the risk assessment are presented to management through a formal risk assessment report. Supplier scorecards have been developed to allow comparison and visibly monitor the performance of our suppliers using a balanced scorecard approach.
STA-05: Supply Chain Management, Transparency and Accountability - Supply Chain Agreements	*Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms:* • *Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and*	Third party security and privacy requirements are established through vendor due-diligence reviews, conducted by the designated Microsoft Azure manager, and included in signed contractual agreements prior to engaging in third party services. The engaging team within Microsoft Azure is responsible for managing their third party relationships, including contract management, monitoring of metrics such as service level agreements, and vendor access to relevant applications.

	support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations) • *Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships* • *Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts* • *Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain)* • *Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed* • *Expiration of the business relationship and treatment of customer (tenant) data impacted* • *Customer (tenant) service-to-service application (API) and data interoperability and portability requirements for application development and information exchange, usage, and integrity persistence*	
STA-06: Supply Chain Management, Transparency and Accountability - Supply Chain Governance Reviews	*Providers shall review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.*	Security risks related to external parties, such as customers, contractors and vendors are identified and addressed through the following: 1. Customer risks are assessed in coordination with LCA and appropriate customer agreements are established. 2. Third parties undergo a review process through Global Procurement and an approved vendor list has been established. Purchase orders to engage a third-party require an MMVA to be established or a review to be

		performed by LCA. Vendors requiring access to source code need to be approved by the GM and LCA, and sign a Source Code Licensing Agreement. 3. Additional risks related to granting access to facilities and information systems are controlled and managed by Microsoft internal IT. Physical and network security for offsite vendor facilities are governed by Microsoft.
STA-07: Supply Chain Management, Transparency and Accountability - Supply Chain Metrics	*Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream).* *Reviews shall performed at least annually and identity non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.*	Microsoft Azure has established procedures and designated responsibilities for managing changes to third-party services. Microsoft Azure 's designated teams manage third-party relationships including contract management, monitoring metrics such as service-level agreements, and third party access to systems, in accordance with these procedures as well as corporate-wide third party management processes. The services provided by third-party vendors are monitored against the service levels by designated responsible persons in Microsoft Azure , as defined in the Statement of Work (SOW). Procedures for monitoring breaches to contractual obligations and handling issues with vendors are established.
STA-08: Supply Chain Management, Transparency and Accountability - Third Party Assessment	*Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review shall include all partners/third party-providers upon which their information supply chain depends on.*	Microsoft Azure contractually requires that its subcontractors meet important privacy and security requirements. Requirements and contracts are reviewed at least annually or as renewed.
STA-09: Supply Chain Management, Transparency and Accountability - Third Party Audits	*Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.*	The services provided by third-party vendors are monitored against the service levels by designated responsible persons from Azure and contractually requires that its subcontractors meet important privacy and security requirements. Third party service providers are routinely audited by both Microsoft and independent audit teams.

Threat and Vulnerability Management: Controls TVM-01 through TVM-03		
TVM-01: Threat and Vulnerability Management - Anti-Virus / Malicious Software	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.*	When providing the Antimalware solution for Virtual Machines, Azure is responsible for ensuring the service is highly available, definitions are updated regularly, that configuration through the Azure Management Portal is effective and that the software detects and protects against known types of malicious software. MCIO-managed hosts in the scope boundary are scanned to validate anti-virus clients are installed and current signature-definition files exist.
TVM-02: Threat and Vulnerability Management - Vulnerability / Patch Management	*Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g. network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.*	Procedures have been established and implemented to scan for vulnerabilities on MCIO-managed hosts. MCIO implements vulnerability scanning on server operating systems, databases, and network devices with appropriate vulnerability scanning tools. MCIO web applications are scanned with the appropriate scanning solution. Vulnerability scans are performed on a quarterly basis at a minimum. Microsoft Azure contracts with independent assessors to perform penetration testing of the Microsoft Azure boundary. Software updates are released through the monthly OS release cycle using change and release management procedures. Emergency out-of-band security software updates (0-day & Software Security Incident Response Process - SSIRP updates) are deployed as quickly as possible. If customers use the default "Auto Upgrade" option, software updates will be applied to their VMs automatically. Otherwise, customers have the option to upgrade to the latest OS image through the management portal. In the case of a VM role, customers are responsible for evaluating and updating their VMs.
TVM-03: Threat and Vulnerability Management - Mobile Code	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.*	The use of mobile code in Azure applications is reviewed during multiple phases of the SDL process. The SDL policy documents the usage restrictions and implementation guidance on mobile technologies such as ActiveX, Flash, Silverlight and JavaScript. It also lists the outdated technologies that are not permitted in Azure.

Appendix A: Cloud Assurance Challenges

Having a good grasp of risk management is important in today's information security and privacy landscape.

When working with cloud computing providers such as Microsoft Azure and cloud-provided services such as Office 365 and Microsoft Dynamics 365, it is important to understand that risk assessments need to consider the dynamic nature of cloud computing.

An organization needs to consider performing a full-scope risk assessment that looks at several criteria whenever a new initiative is underway. Cloud computing is no different. Some of the more prominent criteria that typically interest organizations that are considering cloud computing deployments are discussed in the following sections.

There are many security dimensions to consider in cloud computing scenarios.

Layers

When evaluating controls in cloud computing, it is important to consider the entire services stack of the cloud service provider. Many different organizations may be involved in providing infrastructure and application services, which increases the risk of misalignment. A disruption of any one layer in the cloud stack, or in the customer-defined last mile of connectivity, could compromise the delivery of the cloud service and have negative impacts. As a result, customers should evaluate how their service provider operates and understand the underlying infrastructure and platforms of the service as well as the actual applications.

Data loss

Cloud computing in its current multi-tenant form is relatively new, and many deploying organizations are concerned with the maturity of the tools used by providers to host and manage their data. Microsoft stands out from newer entrants to the market because of its decades of experience in related technology platforms (such as Hotmail® and MSN®).

Beyond the typical risk of data loss on disk drives, the existence of additional tools such as hypervisors, virtual machine managers, new operating and storage environments, and rapidly deployed applications introduce additional stability and redundancy factors that must be included in data loss considerations.

Data Center Tier

See also Microsoft Global Datacenters

While Microsoft supports the spirit of the Uptime Institute's Availability classifications, which are prescriptive-based for easy adoption by the industry as a whole, we have chosen to use a more performance-based approach that uses science to match the SLAs to the

customer need. Microsoft's data centers are engineered to provide 99.999% availability to meet our customer's SLAs and service needs. Microsoft invests significantly in the global operations, management, networks, and sustainability of our facilities that deliver over 200 online services 24 x 7 x 365. Some of those services you may already know and use today like Bing, Hotmail, MSN, Office 365, Xbox Live and Windows Live, which hosts more than half a billion active IDs each day, in 59 markets and is localized in 36 languages.

As most data center operators know, the physical design of the facility is only part of the equation; Microsoft has invested over $3 billion in building our global facilities and networks and over $9 billion in research and development to continue to build innovation and efficiency in our IT solutions. As a result, Microsoft's data centers are evolving at a more rapid pace than many facilities in the industry and thus do not follow the guidelines outlined by Uptime Institute's tier classifications. Therefore, we do not pursue Uptime certification of our facilities. In addition to the wealth of operational insight that comes with running one of the world's largest data center portfolios, Microsoft uses IEEE Gold Book data and third party reliability simulation software to continuously improve our data center design standards. Microsoft's global data center portfolio enables us to deliver the right data center capability at the right time to match the specific service needs of our every day.

Generation 1, 2 and 3 facilities are designed to deliver 99.999% availability to meet our customer's SLAs and service needs. These facilities are fault tolerant and currently maintainable – meaning that while critical components are being maintained, we can still absorb an outage of another critical component. These data centers include:

- Amsterdam (Generation 2)
- Chicago Colocation Rooms (Generation 3)
- Dublin 3 (Generation 3)
- Japan (Generation 1)
- San Antonio 1&2 (Generation 2)
- Quincy 1&2 (Generation 2)

Generation 4 facilities are designed to deliver 99.999% availability. They significantly reduce infrastructure and IT complexity, and allow us to compartmentalize risk depending on application priorities. If an outage occurs simultaneously with maintenance, we have built capabilities into the distribution that limit potential server failure to a subset of one colocation area. Considerable engineering effort has gone into our Generation 4 facilities to simplify operation and minimize opportunities for human error. These data centers include:

- Boynton 1 (Generation 4), Dublin 4 (Generation 4) , Des Moines 1 (Generation 4)

Privacy

As part of the security risk assessment, a privacy review needs to be considered to ascertain potential risks to the data and operations in the cloud. Today, the notion of privacy goes beyond the traditional description of customer data and extends into *organizational* privacy, which includes most intellectual property constraints; that is, the know-how, know-why, and know-when of organizations. As more and more organizations become knowledge-based, the intellectual property values that they generate increase. In fact, intellectual property value is often a significant part of an organization's value.

Confidentiality and integrity

Similarly, concerns about *confidentiality* (who can see the data) and *integrity* (who can modify the data) are important to include in any evaluation. Generally, the more access points to the data, the more complicated the risk profile creation process. Although many regulatory frameworks focus on confidentiality, others such as Sarbanes-Oxley focus almost exclusively on the integrity of data that is used to produce report financial statements.

Reliability

In many cloud computing environments, the data flow that moves information into and out of the cloud must be considered. Sometimes multiple carriers are involved, and oftentimes access beyond the carrier must be evaluated. For example, a failure at a communications service provider can cause delay and affect the reliability of cloud-based data and services. Any additional service provider must be evaluated and assessed for risk.

Auditing, assurance, and attestation

Many organizations are experienced in traditional application and data deployment activities, such as auditing and assessments. In a cloud deployment, the need for some of these activities becomes even more acute at the same time that the activities themselves become more complex.

Embedded in the cloud concept, and especially in public cloud deployment, is a lack of physical control by the organization that owns the data. Physical controls must be considered to protect the disk drives, the systems, and even the data centers in which data resides. Such considerations also apply to software environments in which cloud services components are deployed.

In addition, obtaining permissions for the purpose of satisfying requirements for resiliency testing, penetration testing, and regular vulnerability scanning can be a challenge in cloud deployments.

For certain regulatory frameworks, auditing is a requirement. Frequently, cloud customers are faced with challenges that threaten or appear to deny the many benefits of cloud adoption and deployment.