Microsoft Azure Responses to Cloud Security Alliance Consensus Assessments Initiative Questionnaire v3.0.1

Microsoft

http://www.microsoft.com/trust

NOTE: Certain recommendations contained herein may result in increased data, network, or compute resource usage, and increase your license or subscription costs.

Version 1, Published March 2016

Table of Contents

1 Introduction

The Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire (CAIQ) v3.0.1 provides a comprehensive set of questions that customers can use to evaluate the depth / breadth of cloud vendors' security, privacy, and compliance processes. The Microsoft Azure team has compiled detailed responses to the ~300 items in the assessment, laid out in the following sections according to their respective domains.

If you're contemplating a move to the public cloud, or are already in the midst of your migration, this document will be a valuable resource for understanding how Azure meets and exceeds the requirements set forth by the CSA. Below you will find information culled from Azure engineering, operations, and policies. In most cases, the responses are specific to Azure, but are identified when broader Microsoft policies apply.

We recommend also reviewing Azure's response to the CSA Cloud Control Matrix (CCM), which is available on the Microsoft Trust Center at http://www.microsoft.com/trust. This document is aligned 1:1 with the CAIQ, and similarly aligns with multiple international standards and compliance frameworks (for more information, see https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/) such as ISO 27001, PCI, and SOC. Microsoft audits against dozens of standards, and additional details can be obtained through the audit reports available from the Service Trust Portal at https://www.microsoft.com/en-us/TrustCenter/STP/default.aspx).

Microsoft Azure Responses to CSA CAIQ v3.0.1

Application and Interface Security: Controls AIS-01 through AIS-04

Control ID in CCM[1]	Consensus Assessment Questions (CCM Version 3.0.1, Final)	Microsoft Azure Response			
		Yes	No	N/A	Notes
AIS-01.1: Application & Interface Security - Application Security	*Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)?*	Y			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-01.2: Application & Interface Security - Application Security	*Do you use an automated source code analysis tool to detect security defects in code prior to production?*	Y			Source code builds are scanned for malware prior to release to production. The Microsoft Anti-Malware Client and Service is installed by default and available for customers to enable in all Azure Cloud Services. The Microsoft Anti-Malware Client and Service is available as an optional security extension in the Virtual Machines platform.
AIS-01.3: Application & Interface Security - Application Security	*Do you use manual source-code analysis to detect security defects in code prior to production?*		N		A Final Security Review (FSR) is performed for software releases prior to production deployment by a designated Security Advisor outside of the Microsoft Azure development team. Web applications are scanned with the PortSwigger Burp Suite scanning solution.

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

AIS-01.4: Application & Interface Security - Application Security	*Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?*	Y			Services provided by third-party vendors are monitored against agreed upon service levels by responsible parties 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 and attested via industry-standard audit processes such as SOC 1 and 2.
AIS-01.5: Application & Interface Security - Application Security	*(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?*	Y			Procedures have been established and implemented to scan for vulnerabilities on hosts in the scope boundary. Vulnerability scanning is performed on server operating systems, databases, and network devices with the QualysGuard vulnerability scanning tool. The vulnerability scans are performed on a quarterly basis at minimum, but Azure security teams employ continuous monitoring processes to detect potential issues on an ongoing basis. Microsoft Azure contracts with independent assessors to perform penetration testing of the Microsoft Azure boundary. Red-Team / Blue-Team exercises (See AIS-01.1) are also routinely performed and results used to make security improvements.
AIS-02.1: Application & Interface Security - Customer Access Requirements	*Are all identified security, contractual and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets and information systems?*	Y			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 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 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. **ISO 27018** Microsoft is the first major cloud provider to adopt the international code of practice for cloud privacy. ISO was developed to establish a uniform, international approach to protecting the privacy of personal data stored in the cloud. The

					British Standards Institution independently verified that Microsoft Azure is aligned with the guideline's code of practice. ISO 27018 controls include a prohibition on the use of customer data for advertising and marketing purposes without the customer's express consent.
AIS-02.2: Application & Interface Security - Customer Access Requirements	*Are all requirements and trust levels for customers' access defined and documented?*	Y			Customer access controls and trust levels are described on the Microsoft Azure Trust Center website at https://www.microsoft.com/en-us/TrustCenter/default.aspx.
AIS-03.1: Application & Interface Security - Data Integrity	*Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?*	Y			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-04.1: Application & Interface Security - Data Security / Integrity	*Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?*	Y			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

Control ID in CCM	Consensus Assessment Questions (CCM Version 3.0.1, Final)	Microsoft Azure Response			
		Yes	No	N/A	Notes
AAC-01.1: Audit Assurance & Compliance - Audit Planning	*Do you produce audit assertions using a structured, industry accepted format (e.g., CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?*	Y			No, however, 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. ISO 27001 certifications for Microsoft Azure and Microsoft Cloud Infrastructure and Operations (MCIO) can be found on the website of our external ISO auditor, the BSI Group. Additional audit information is available under NDA upon request by prospective and existing customers. In addition to providing a high level of assurance that our controls are operating as expected, the compliance framework also results in several important certifications and attestations for Microsoft's cloud infrastructure, including ISO/IEC 27001:2013 certification, SSAE 16/ISAE 3402 SOC 1 Type 1 and Type 2 and AT Section 101 SOC 2 and 3 Type 1 and Type 2 attestations, as well as FedRAMP Certification and Accreditation.
AAC-02.1: Audit Assurance & Compliance - Independent Audits	*Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?*	Y			ISO 27001 certifications for Microsoft Azure and MCIO can be found on 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. Customers can also review SOC, ISO, PCI, and other audit reports directly through the Microsoft Service Trust Portal at http://aka.ms/audits.
AAC-02.2: Audit Assurance & Compliance - Independent Audits	*Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?*	Y			As defined in AIS-01.1, regular scans, conducted at least quarterly, are conducted against the Azure infrastructure and applications using a variety of commercial and proprietary scanning tools. Critical and High findings detected are reviewed and patched per the Change and Release Management Policy. Rescans are conducted within 30 days. 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 restoration.

AAC-02.3: Audit Assurance & Compliance - Independent Audits	*Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?*	Y			Scans are performed by MCIO security professionals on behalf of Microsoft Azure. Penetration testing methodologies for Infrastructure and Applications are defined and are based on a combination of common criteria, NIST SP800-115, ETSI, OWASP, IETF and ISO 27000. To protect Azure platform services, Microsoft provides a distributed denial-of-service (DDoS) defense system that is part of Azure's continuous monitoring process, and is continually improved through scheduled penetration-testing and Red-Team exercises. Azure's DDoS defense system is designed to mitigate attacks from the outside and also from other Azure tenants. The Azure DDoS defense technology provides detection and mitigation techniques such as SYN cookies, rate limiting, and connection limits to help ensure that such attacks do not impact customer environments.
AAC-02.4: Audit Assurance & Compliance - Independent Audits	*Do you conduct internal audits regularly as prescribed by industry best practices and guidance?*	Y			Internal audits required to satisfy industry best practices, regulatory requirements and compliance requirements are conducted at the recommended intervals. Microsoft Azure complies with and audits against ISO 27001 controls in order to ensure that compliance is independently verified. The purpose of the internal audits is to assess conformance to the requirements of ISO 27001 and relevant legislation or regulations and to verify the identified information security requirements are effectively implemented and maintained.
AAC-02.5: Audit Assurance & Compliance - Independent Audits	*Do you conduct external audits regularly as prescribed by industry best practices and guidance?*	Y			Yes. Microsoft conducts audits and assessments against a growing number of US, international, and industry standards and frameworks. These include PCI DSS, SOC, ISO, IRAP, CDSA, MTCS, FedRAMP, DISA, and many others. More details about Azure's current portfolio of certifications can be found at the Azure Trust Center website.
AAC-02.6: Audit Assurance & Compliance - Independent Audits	*Are the results of the penetration tests available to tenants at their request?*	Y			Yes, summary penetration testing reports are available to customers under NDA. For more information, visit the Microsoft Azure Trust Center, or contact your Microsoft account representative.
AAC-02.7: Audit Assurance & Compliance - Independent Audits	*Are the results of internal and external audits available to tenants at their request?*	Y			The results of external audits are available publically on the Microsoft Azure Trust Center website; and some details of these reports are additionally available to customers with a signed NDA. Internal audits and their findings may contain sensitive information and are not made available.
AAC-02.8: Audit Assurance & Compliance - Independent Audits	*Do you have an internal audit program that allows for cross-*	Y			Microsoft conducts a variety of regular internal audits that are utilized in multiple different security and compliance assessments.

	functional audit of assessments?				
AAC-03.1: Audit Assurance & Compliance - Information System Regulatory Mapping	*Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?*	Y			Customer environments and data in Azure are isolated using numerous mechanisms, technologies, policies, processes, and architectural elements. Among these are (but not limited to): Virtual Networks--customer tenants and VM deployments are kept logically separated through VNets that define DNS, security policies, and IP routing rules. Firewalls, ACLs, Network Security Groups, IP Filters, Virtual appliances, Load Balancers, and network policies work together to prevent unauthorized traffic from entering or leaving a customer's tenant, either across network boundaries or between the virtualization host and guest. Encryption--customer data is encrypted in-transit and at-rest through configurable and standards-based providers using a variety of protocols. This includes BitLocker, AES-256 (in Azure Media Services), IPsec (VNets), etc. Access Control--Azure Storage, the Azure Portal, and other service components provide role-based access controls and key-based authentication to help ensure only authorized entities can gain access to tenant data. The concept of tenant containers is maintained in the Azure Active Directory service at multiple layers, from portals to persistent storage. These boundaries ensure a query scoped to a given tenant never returns directory data for another tenant. Front ends (Azure AD Sync, PowerShell, Graph) all store and retrieve data through an internal directory services API (DSAPI) which calls an authorization layer to ensure the data requested is allowed for the user requesting the data. All of these capabilities are available to customers for isolating and protecting their data, gaining access to only their data and no others'.
AAC-03.2: Audit Assurance & Compliance - Information System Regulatory Mapping	*Do you have capability to recover data for a specific customer in the case of a failure or data loss?*	Y			Azure Storage automatically replicates your data to help guard against unexpected hardware failures and ensure that your data is available when you need it. Azure keeps 3 copies within a single region. For higher availability and disaster recovery, optional geo-redundancy creates 3 additional copies hundreds of miles away. When you create a storage account, you must select one of the following replication options: • **Locally redundant storage (LRS)** replicates your data within the region in which you created your storage account. To maximize durability, every request made against data in your storage account is replicated three times. These three replicas each reside in separate fault domains and upgrade domains.

					• **Zone-redundant storage (ZRS)** replicates your data across two to three facilities, either within a single region or across two regions, providing higher durability than LRS. If your storage account has ZRS enabled, then your data is durable even in the case of failure at one of the facilities. • **Geo-redundant storage (GRS)** replicates your data to a secondary region that is hundreds of miles away from the primary region. If your storage account has GRS enabled, then your data is durable even in the case of a complete regional outage or a disaster in which the primary region is not recoverable. • **Read-access geo-redundant storage (RA-GRS)** providing read-only access to the data in the secondary location, in addition to the replication across two regions provided by GRS. In the event that data becomes unavailable in the primary region, your application can read data from the secondary region.
AAC-03.3: Audit Assurance & Compliance - Information System Regulatory Mapping	*Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?*	Y			Most Azure services are deployed regionally and enable the customer to specify the region of the Microsoft datacenter in which customer data will be stored, i.e. virtual machines, storage, and SQL Database. Data and VMs may be geo-tagged to prevent migration to locations not desired by the tenant. Data in Azure is stored in Microsoft datacenters around the world based on the geo-location properties specified by the customer using the Microsoft Azure Portal.
AAC-03.4: Audit Assurance & Compliance - Information System Regulatory Mapping	*Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?*	Y			Microsoft takes a two-pronged approach to help ensure that compliance controls are current and that we build and maintain a dynamic compliance framework. First, a team of Microsoft experts works with our engineering and operations teams, as well as external regulatory bodies, to track existing standards and regulations, developing hundreds of controls for our product teams to build into our cloud services. Second, because regulations and standards are always evolving, our compliance experts also anticipate upcoming changes to help ensure continuous compliance—researching draft regulations, assessing potential new requirements, and developing corresponding controls. This approach to designing compliance controls helps ensure that they operate effectively, with stringent safeguards.

Business Continuity Management and Operational Resilience: Controls BCR-01 through BCR-11

Control ID in CCM	Consensus Assessment Questions (CCM Version 3.0.1, Final)	Microsoft Azure Response			
		Yes	No	N/A	Notes
BCR-01.1: Business Continuity Management & Operational Resilience - Business Continuity Planning	*Do you provide tenants with geographically resilient hosting options?*	Y			Yes. Most Azure services within larger geographies are deployed regionally and enable the customer to specify the region of the Microsoft datacenter in which customer data will be stored. The United States has 6 regions; Europe has 2 regions; Asia Pacific has 2 regions; Japan has two regions; Brazil has 1 region; and Australia has 2 regions. Azure creates three copies of data in the region configured by the customer and offers geo-replication in a datacenter hundreds of miles away within the same region.
BCR-01.2: Business Continuity Management & Operational Resilience - Business Continuity Planning	*Do you provide tenants with infrastructure service failover capability to other providers?*		N		No, however, tenants have multiple options within the Azure platform to ensure workloads and data can have redundancy through mirroring and cold standby database failover capabilities, and interoperability with third party backup services if the customer so chooses.
BCR-02.1: Business Continuity Management & Operational Resilience - Business Continuity Testing	*Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?*	Y			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 (RPO) 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-03.1: Business Continuity Management & Operational Resilience - Datacenter Utilities /	*Do you provide tenants with documentation showing the transport route of their data between your systems?*	Y			Physical network diagrams are maintained for all Azure datacenters, with general data flow indicated in the System Descriptions that accompany the SOC 1, 2 and 3 audit reports. These diagrams provide functional level detail on load balancers, routers, firewalls, and other network infrastructure. SOC audit reports are available to customers under NDA from http://aka.ms/stphelp.

Environmental Conditions					
BCR-03.2: Business Continuity Management & Operational Resilience - Datacenter Utilities / Environmental Conditions	*Can tenants define how their data is transported and through which legal jurisdictions?*	Y			Customers may specify the geographic areas ("geos" and "regions") of the Microsoft datacenters in which their customer data will be stored, which allows for data being maintained in a particular jurisdiction. For example, to allow for the continuous flow of information required by international business (including the cross-border transfer of personal data), Microsoft offers customers EU Standard Contractual Clauses that provide additional contractual guarantees around transfers of personal data for in-scope services. Our implementation of the EU Model Clauses has been validated by EU data protection authorities as being in line with the rigorous privacy standards that regulate international data transfers by companies operating in its member states. Microsoft was the first company to receive approval from the EU's Article 29 Working Party for its strong contractual commitments to comply with EU privacy laws no matter where data is located.
BCR-04.1: Business Continuity Management & Operational Resilience - Documentation	*Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?*	Y			Extensive documentation, including operating procedures, security and hardening guides, diagrams, and system build documentation is maintained in a secure internal site and made available to authorized personnel. In addition, Microsoft Azure has established Security on-boarding SharePoint sites, assigned Privacy Champions 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-05.1: Business Continuity Management & Operational Resilience - Environmental Risks	*Is physical protection against damage (e.g., natural causes, natural disasters, deliberate attacks) anticipated and designed with countermeasures applied?*	Y			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 27001) for physical security and availability. They are managed, monitored, and administered by Microsoft operations personnel.

BCR-06.1: Business Continuity Management & Operational Resilience - Equipment Location	*Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?*		N		Microsoft data center site selection is performed using a number of criteria, including mitigation of environmental risks. In areas where the exists a higher probability of earthquakes, seismic bracing of the facility is employed. Data centers are built as redundant, highly-available components of the Azure platform. 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-07.1: Business Continuity Management & Operational Resilience - Equipment Maintenance	*If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?*	Y			Underlying virtual hard disks (.vhd files) used by virtual machines are kept in Blob storage in an Azure storage account. 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. Resource allocation is managed by Azure Fabric Controllers; Azure provides a combination of resource management, elasticity, load balancing, and partitioning to enable high availability. Azure services have redundant components; if one experiences a hardware failure or must be temporarily taken down to upgrade its software, the service remains available through other instances.
BCR-07.2: Business Continuity Management & Operational Resilience - Equipment Maintenance	*If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?*	Y			Azure Backup provides the ability to back up and restore virtual machines. When the process to discover virtual machines in a region is initiated, a one-time registration is performed to install the backup extension, then a backup and retention policy is defined for each VM. From that point forward, replication and incremental backup is automatically performed. Once backed up, a VM can be restored from the latest recovery point or older, restore to an existing or new cloud service, and specify the virtual network and subnet for the restored VM.
BCR-07.3: Business Continuity Management & Operational Resilience - Equipment Maintenance	*If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?*	Y			Within PowerShell, the Export-AzureVM command exports the state of an Azure virtual machine to a file. You can also use Azure Import/Export service to transfer large quantities of data resident in Blob storage to your on-premises installations.

BCR-07.4: Business Continuity Management & Operational Resilience - Equipment Maintenance	*If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?*	Y			Customers may export virtual hard disk files and store those images outside of Azure.
BCR-07.5: Business Continuity Management & Operational Resilience - Equipment Maintenance	*Does your cloud solution include software/provider independent restore and recovery capabilities?*	Y			Tenants may use Azure Backup or StorSimple, which are services available to Azure customers, or they may utilize independent third party provider backup solutions to locations outside of the Azure platform.
BCR-08.1: Business Continuity Management & Operational Resilience - Equipment Power Failures	*Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?*	Y			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. More importantly, we are continuously investing in developing greater application resiliency in our software so it will instantly recognize a disruption and gracefully failover to a different set of servers or even a different datacenter, without interrupting the availability of the service. Azure data centers 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 data centers have made arrangements for emergency fuel delivery. Data centers also have a dedicated Facility Operations Center to monitor the following: Power systems, including all critical electrical components – generators, transfer switch, main switchgear, power management module and uninterruptible power supply equipment.
BCR-09.1: Business Continuity Management & Operational Resilience - Impact Analysis	*Do you provide tenants with ongoing visibility and reporting of your operational Service Level*	Y			Microsoft requires that customers submit an SLA breach claim to customer support by the end of the calendar month after the event has happened. (For example, if an incident happens in mid-February, the customer has until the end of March to report it.) The claim must include: a detailed description of the incident; duration of incident; number of users or sites impacted; description of your attempts to remedy the situation.

	Agreement (SLA) performance?				See also https://azure.microsoft.com/en-us/status/ for current status across all Azure datacenters and services.
BCR-09.2: Business Continuity Management & Operational Resilience - Impact Analysis	*Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?*	Y			The security logs in Microsoft Azure Cloud Services and Virtual Machines contain vital information that can provide intelligence and insights into the following security issues including, policy violations, internal and external threats, regulatory compliance and network, host, and user activity anomalies. Customers can then use HDInsight to aggregate and analyze the collected events. In addition, these collected events can be exported to on-premises security information and event management (SIEM) systems for ongoing monitoring.
BCR-09.3: Business Continuity Management & Operational Resilience - Impact Analysis	*Do you provide customers with ongoing visibility and reporting of your SLA performance?*	Y			Logs for primary operations related to your Azure subscription resources are also available through the Operation Logs feature in the Azure management portal. Microsoft monitors SLA performance and notifies customers if there is a lapse.
BCR-10.1: Business Continuity Management & Operational Resilience - Policy	*Are policies and procedures established and made available for all personnel to adequately support services operations' roles?*	Y			Management has established roles and responsibilities to oversee implementation of the information security policy across Microsoft Azure. Microsoft Azure management is responsible for overseeing security within their respective teams (including third parties), and facilitating compliance with security policies, processes and standards. In addition, Azure has established a Security on-boarding SharePoint site, assigned Privacy Champions 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. An Enterprise Business Continuity Management (EBCM) framework has been established for Microsoft and applied to individual business units including the Cloud and Enterprise (C&E) division under which 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; and • Training and Awareness.
BCR-11.1: Business Continuity Management & Operational Resilience - Retention Policy	*Do you have technical control capabilities to enforce tenant data retention policies?*	Y			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, but Azure provides a 90-day window for subscription and storage account deletion to prevent accidental data loss. Microsoft Azure provides tools to securely delete data including immediately removing the index from the primary location removal of any geo-replicated copy of the data (index) asynchronously, wiping is NIST 800-88 compliant, defective disks are destroyed, and customers can only read from disk space to which they have previously written.
BCR-11.2: Business Continuity Management & Operational Resilience - Retention Policy	*Do you have a documented procedure for responding to requests for tenant data from governments or third parties?*	Y			Microsoft does not provide any government with direct or unfettered access to customer data. Microsoft releases only specific data mandated by the relevant legal demand. If a government wants customer data—including for national security purposes—it needs to follow the applicable legal process, meaning it must serve us with a court order for content or a subpoena for account information. If compelled to disclose customer data, we will promptly notify you and provide a copy of the demand, unless legally prohibited from doing so. We respond only to requests for specific accounts and identifiers. There is no blanket or indiscriminate access to Microsoft's customer data. Every request is explicitly reviewed by Microsoft's legal team, which ensures that the requests are valid, rejects those that are not, and makes sure that we provide only the data specified in the order. In its commitment to transparency, Microsoft regularly publishes a Law Enforcement Requests Report that discloses the scope and number of government requests we receive. It is worth noting that the aggregate data we have published shows clearly that only a tiny fraction—fractions of a percent—of our customers have ever been subject to a government demand related to criminal law or national security. For enterprise customers, these numbers drop further to a mere handful.

					These privacy commitments are backed by Microsoft's adoption of the world's first international code of practice for cloud privacy, ISO/IEC 27108, in February 2015—the first major cloud provider to do so.
BCR-11.3: Business Continuity Management & Operational Resilience - Retention Policy	*Have you implemented backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?*	Y			Microsoft Azure backs up infrastructure data regularly and validates restoration of data periodically for disaster recovery purposes. Backup standards and policies, procedures and controls are verified, documented and audited both internally and by third party assessors.
BCR-11.4: Business Continuity Management & Operational Resilience - Retention Policy	*Do you test your backup or redundancy mechanisms at least annually?*	Y			Yes, as defined in the Azure Business Continuity and Disaster Recovery Standard Operating Procedure.
BCR-11.5: Business Continuity Management & Operational Resilience - Retention Policy	*Do you have technical control capabilities to enforce tenant data retention policies?*	Y			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, but Azure provides a 90-day window for subscription and storage account deletion to prevent accidental data loss. Microsoft Azure provides tools to securely delete data including immediately removing the index from the primary location removal of any geo-replicated copy of the data (index) asynchronously, 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

Control ID in CCM	Consensus Assessment Questions (CCM Version 3.0.1, Final)	Microsoft Azure Response			
		Yes	No	N/A	Notes
CCC-01.1: Change Control & Configuration Management - New Development / Acquisition	*Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?*	Y			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 improving 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 Customers are responsible for their own applications hosted in Microsoft Azure.
CCC-01.2: Change Control & Configuration Management - New Development / Acquisition	*Is documentation available that describes the installation, configuration and use of products/services/features?*	Y			Extensive documentation is available in the form of websites, whitepapers, Microsoft employee blog entries and video tutorials that describes the installation, configuration and use of products and features on the Azure website. Reference websites provide the most current information, documentation, video-on-demand, and procedures for configuring services in Compute, Web & Mobile, Data & Storage, Analytics and Networking.

CCC-02.1: Change Control & Configuration Management - Outsourced Development	*Do you have controls in place to ensure that standards of quality are being met for all software development?*	Y			External business partners 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. Microsoft also adheres to the SD3+C principle of development: Secure by design; Secure by default; secure in deployment and communications. Azure is also audited against the controls in the NIST 800-53 risk management framework which encompass quality control for FedRAMP.
CCC-02.2: Change Control & Configuration Management - Outsourced Development	*Do you have controls in place to detect source code security defects for any outsourced software development activities?*	Y			The Security Development Lifecycle (SDL) is a software development process that helps developers build more secure software and address security compliance requirements while reducing development cost. Any outsourced software development follows the same controls and processes listed in CCC-01.1 and Microsoft Azure software changes are reviewed for unauthorized changes and defects through Security Development Lifecycle (SDL) change and release management processes.
CCC-03.1: Change Control & Configuration Management - Quality Testing	*Do you provide your tenants with documentation that describes your quality assurance process?*	Y			Operational Security Assurance (OSA) is 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 data centers 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 service 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 all requirements to establish the OSA baseline requirements. - Engaging and implementing the new requirements and baselines. Customers also have access to third party audit reports and certifications that encompass the controls relevant to security in development and support processes which encompass quality assurance.
CCC-03.2: Change Control & Configuration Management - Quality Testing	*Is documentation describing known issues with certain products/services available?*	Y			Documentation of known issues with products and services are available at the Microsoft support website and within the Azure reporting platform.
CCC-03.3: Change Control & Configuration Management - Quality Testing	*Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?*	Y			Microsoft Azure identifies, reports, and corrects bugs and vulnerabilities through its incident response, vulnerability management and configuration management processes. Software updates to correct flaws are tested throughout the SDL process.
CCC-03.4: Change Control & Configuration Management - Quality Testing	*Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?*	Y			Prior to release to production, software code is inspected and reviewed during the quality assurance phase to ensure it is consistent with the approved build release. The engineer submits the code review to the internal review service, which creates the package of the changes and submits them for review. Project teams perform security testing in the implementation, verification and release phases of the Microsoft SDL process, including by employing automated code scanning and security tools to identify flaws and weaknesses in software. The identified flaws and vulnerabilities are formally tracked and remediated. When the code review is submitted, the system sends an email to the assigned reviewers and posts the code on the review site. An internal website is used as the hub for code submitted for review. As reviewers complete their reviews the details are stored on the server and the code owner is notified. Once approved, the code is queued.
CCC-04.1: Change Control & Configuration Management - Unauthorized Software Installations	*Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?*	Y			All changes into production go through the Change Management process described in CCC-01. This process also requires that: - Pre-screened admin requests from Microsoft corporate networks are approved - That role-based and Just-in-Time access controls are enforced - Privileges issued are temporary and grant the least privilege required to complete task (just-enough access)

					- Multi-factor authentication for all administrative access is required - All access requests are logged and audited Microsoft Azure source code libraries are limited to authorized personnel. 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. "Access control and access control to program source code" is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 11 and 12.4.3. For more information, review of the publicly available ISO standards we are certified against is suggested.
CCC-05.1: Change Control & Configuration Management - Production Changes	*Do you provide tenants with documentation that describes your production change management procedures and their roles / rights / responsibilities within it?*	Y			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

Control ID in CCM	Consensus Assessment Questions (CCM Version 3.0.1, Final)	Microsoft Azure Response			
		Yes	No	N/A	Notes
DSI-01.1: Data Security & Information Lifecycle Management - Classification	*Do you provide a capability to identify virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?*		N		Microsoft 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.
DSI-01.2: Data Security & Information Lifecycle Management - Classification	*Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?*		N		All hardware is uniquely identified using software monitoring tools and hardware asset tags as part of the Azure Data Classification program. This data is not available to customers.
DSI-01.3: Data Security & Information Lifecycle Management - Classification	*Do you have a capability to use system geographic location as an authentication factor?*	Y			While geo-location cannot solely be used as an authentication factor, authentication can be restricted through the application of access control lists by IP addresses in specific geographies. Customers can generate reports from Azure AD and view anomalous login activity that could indicate a remote hacking attempt.
DSI-01.4: Data Security & Information Lifecycle Management - Classification	*Can you provide the physical location/geography of storage of a tenant's data upon request?*		N		Data in Microsoft Azure is stored in Microsoft datacenters around the world based on the geo-location properties specified by the customer using the Microsoft Azure Portal. While Azure can verify the geo or region in which data is located, it cannot provide the specific server or data center upon customer request.

DSI-01.5: Data Security & Information Lifecycle Management - Classification	*Can you provide the physical location / geography of storage of a tenant's data in advance?*	Y			Most Azure services permit customers to specify the particular geography where their customer data will be stored. Data may be replicated within a selected geographic area or region for redundancy, but it will not be replicated outside of it unless specifically configured so by the customer.
DSI-01.6: Data Security & Information Lifecycle Management - Classification	*Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?*	Y			Microsoft Azure classifies and labels data according to the Microsoft Azure data classification scheme and then implements a standard set of Security and Privacy attributes. Information classification, labeling and handling is covered under the ISO 27001:2013 standards, specifically addressed in domain 8.2.2.
DSI-01.7: Data Security & Information Lifecycle Management - Classification	*Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?*	Y			Most Azure services permit customers to specify the particular geography where their customer data will be stored and where their virtual machines are deployed. Virtual Networks (VNETS) may also span an entire region.
DSI-02.1: Data Security & Information Lifecycle Management - Data Inventory / Flows	*Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?*	Y			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 backup 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; -- Azure RemoteApp, which may store end user names and device IP addresses globally, depending on where the end user accesses the service.

DSI-02.2: Data Security & Information Lifecycle Management - Data Inventory / Flows	*Can you ensure that data does not migrate beyond a defined geographical residency?*	Y			Customers may specify the geo and region of the Microsoft datacenters where their data will be stored. Microsoft will not transfer data outside the geo(s) specified by the customer except where necessary for Microsoft to provide customer support, troubleshoot the service, or comply with legal requirements; or where the customer configures the account to enable the transfer of data, including through the use of features that don't enable geo selection or certain other features which may store data globally. A customer can access its data from any geo.
DSI-03.1: Data Security & Information Lifecycle Management - e-Commerce Transactions	*Do you provide open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?*	Y			Transactions involving the Microsoft Azure Portal, including purchase of services, is encrypted using TLS 1.2 256-bit encryption. SSL/TLS is mandatory when accessing the Azure Portal or System Management API (SMAPI). Microsoft Azure complies with PCI-DSS standards and completes an annual PCI audit by an independent, 3rd party PCI-DSS Qualified Security Assessor company. Azure customers are entirely responsible for protection and encryption of their e-commerce transactions, however, Azure ensures critical communications such as calls to the API or intra-Microsoft Azure communication are encrypted, authenticated, and integrity controlled via protocols such as SSL. Customers can optionally configure SSL/TLS for defense-in-depth on their Virtual Networks. Storage REST API over HTTPS can also be used to interact with Azure Storage and Azure SQL Database. When populating data into Azure SQL Database, you can encrypt information before it is copied over, or you can use Column Level Encryption / Transparent Data Encryption within the Azure SQL Database service. Note that data only remains encrypted until it is used and placed in memory on the Azure SQL Database compute node, at which point it exists in an unencrypted state.
DSI-03.2: Data Security & Information Lifecycle Management - e-Commerce Transactions	*Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?*	Y			For data in transit, customers can enable encryption for traffic between their own VMs and end users. Azure protects data in transit, such as between two virtual networks. Azure uses industry standard transport protocols such as TLS between devices and Microsoft data centers, and within data centers themselves.

DSI-04.1: Data Security & Information Lifecycle Management - Handling / Labeling / Security Policy	*Are policies and procedures established for labeling, handling and the security of data and objects that contain data?*	Y			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. 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. All employees, contractors and third parties responsible for managing and maintaining assets must ensure that assets are handled securely and provided with appropriate level of protection.
DSI-04.2: Data Security & Information Lifecycle Management - Handling / Labeling / Security Policy	*Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?*	Y			Media and assets are marked as having a high/medium/low business impact which determines the level of security controls and handling procedures applicable. All media and assets are labeled without exception.
DSI-05.1: Data Security & Information Lifecycle Management - Non-Production Data	*Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?*	Y			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-06.1: Data Security & Information Lifecycle Management - Ownership / Stewardship	*Are the responsibilities regarding data stewardship defined, assigned, documented and communicated?*	Y			MCIO assets have a designated owner who is responsible for asset classification and protection in accordance with classification. 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. 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.

					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.
DSI-07.1: Data Security & Information Lifecycle Management - Secure Disposal	*Do you support secure deletion (e.g., degaussing / cryptographic wiping) of archived and backed-up data as determined by the tenant?*	Y			Microsoft uses best practice procedures and a 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. All 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.
DSI-07.2: Data Security & Information Lifecycle Management - Secure Disposal	*Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?*	Y			Access to administer Microsoft Azure Active Directory portal/services is restricted based on assigned privileges and associated subscription of the customer account. When approved for deletion, the procedures outlined in DSI-07.1 are followed to remove customer data. See also http://blogs.msdn.com/b/walterm/archive/2012/02/01/windows-azure-data-cleansing-and-leakage.aspx.

Datacenter Security: Controls DCS-01 through DCS-09

Control ID in CCM	Consensus Assessment Questions (CCM Version 3.0.1, Final)	Microsoft Azure Response			
		Yes	No	N/A	Notes
DCS-01.1: Datacenter Security - Asset Management	*Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset?*	Y			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. Asset owners are responsible for maintaining up-to-date information regarding their assets.
DCS-01.2: Datacenter Security - Asset Management	*Do you maintain a complete inventory of all of your critical supplier relationships?*	Y			All critical supplier relationships are documented and reviewed at least annually or as changes occur to the relationship.
DCS-02.1: Datacenter Security - Controlled Access Points	*Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) implemented?*	Y			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. All data centers 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 data centers 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. Microsoft data centers all receive SSAE16/ISAE 3402 Attestation and are ISO 27001 Certified
DCS-03.1: Datacenter Security - Equipment Identification	*Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?*	Y			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 of device configuration by comparing them against the defined policies. MCIO turns off the 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-04.1: Datacenter Security - Off-Site Authorization	*Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location to another? (e.g., offsite backups, business continuity failovers, replication)*	Y			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-05.1: Datacenter Security - Off-Site Equipment	*Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment?*	Y			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-06.1: Datacenter Security - Policy	*Can you provide evidence that policies, standards and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas?*	Y			Microsoft Information 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 all 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 Data Centers. 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. All guests are required to wear guest badges and be escorted by authorized Microsoft personnel.

DCS-06.2: Datacenter Security - Policy	*Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards and procedures?*	Y			All appropriate Microsoft employees take part in a Microsoft Azure 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. Microsoft also has non-disclosure provisions in our employee contracts. All Microsoft Azure contractor staff and MCIO staff are required to take any training determined to be appropriate to the services being provided and the role they perform.
DCS-07.1: Datacenter Security - Secure Area Authorization	*Do you allow tenants to specify which of your geographic locations their data is allowed to move into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)?*	Y			Customers may specify the geo and region of the Microsoft datacenters where their data will be stored. Microsoft will not transfer data outside the geo(s) specified by the customer except where necessary for Microsoft to provide customer support, troubleshoot the service, or comply with legal requirements; or where the customer configures the account to enable the transfer of data, including through the use of features that don't enable geo selection or certain other features which may store data globally. A customer can access its data from any geo. Datacenter entrances are guarded 24x7x365 by security personnel and access is controlled through security personnel, authorized badges, locked doors and CCTV monitoring.
DCS-08.1: Datacenter Security - Unauthorized Persons Entry	*Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?*	Y			Azure Employees and contractors must have a business need to enter a Microsoft data center 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-09.1: Datacenter Security - User Access	*Do you restrict physical access to information assets and functions by users and support personnel?*	Y			Access to all 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 Data Centers. 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 and all guests be escorted by authorized Microsoft personnel.

Encryption and Key Management: Controls EKM-01 through EKM-04

Control ID in CCM	Consensus Assessment Questions (CCM Version 3.0.1, Final)	Microsoft Azure Response			
		Yes	No	N/A	Notes
EKM-01.1: Encryption & Key Management - Entitlement	*Do you have key management policies binding keys to identifiable owners?*	Y			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 Azure service. Azure provides each subscription with an associated logical certificate store that enables automatic deployment of service-specific certificates, and to which customers can upload their own. Certificates used in Azure are x.509 v3 certificates and can be signed by another trusted certificate or they can be self-signed. The certificate store is independent of any hosted service, so it can store certificates regardless of whether they are currently being used by any of those services. These certificates and other credentials uploaded to Azure are stored in encrypted form.
EKM-02.1: Encryption & Key Management - Key Generation	*Do you have a capability to allow creation of unique encryption keys per tenant?*	Y			Using Azure Key Vault, tenants can encrypt keys and secrets (such as authentication keys, storage account keys, data encryption keys, .PFX files, and passwords) by using keys that are protected by hardware security modules (HSMs). For added assurance, you can import or generate keys in HSMs (keys never leave the HSM boundary). HSMs are certified to FIPS 140-2 level 2.
EKM-02.2: Encryption & Key Management - Key Generation	*Do you have a capability to manage encryption keys on behalf of tenants?*	Y			Through the use of Key Vault, Azure provides a service for customers to manage and safeguard their cryptographic keys used by cloud applications. Key Vault allows encrypts keys and secrets, such as authentication keys, storage account keys, data encryption keys, .PFX files, and passwords, by using keys that are protected by hardware security modules (HSMs). HSMs are certified to FIPS 140-2 level 2.
EKM-02.3: Encryption & Key Management - Key Generation	*Do you maintain key management procedures?*	Y			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.
EKM-02.4: Encryption & Key Management - Key Generation	*Do you have documented ownership for each stage of the lifecycle of encryption keys?*	Y			Azure customers may use Key Vault to manage their own cryptographic keys while Azure provides the secure hardware platform. Customers can: - Create or import a key or secret - Revoke or delete a key or secret - Authorize users or applications to manage or use keys and secrets

					- Configure key usage (for example, sign or encrypt) - Monitor key usage 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 Azure service. For internal corporate data and transmission encryption, Microsoft has established procedures to manage cryptographic keys throughout their lifecycle (e.g., generation, distribution, revocation). Microsoft Azure uses Microsoft's corporate PKI infrastructure.
EKM-02.5: Encryption & Key Management - Key Generation	*Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?*		N		The Azure Key vault is a cryptographic key management service based on FIPS-validated hardware security modules.
EKM-03.1: Encryption & Key Management - Sensitive Data Protection	*Do you encrypt tenant data at rest (on disk/storage) within your environment?*	Y			Microsoft Azure does not encrypt all tenant data in storage by default. However, there are tools within Azure and third party tools that allow encryption of data in Azure storage. Customers may implement encryption at rest using .NET cryptographic services and BitLocker (for full volume encryption). For customers using Virtual Machines, additional options are available, including the Encrypting File System in Windows Server 2008 R2 (and above), Azure Rights Management Services, as well as Transparent Data Encryption (TDE) in SQL Server 2008 R2 (and above). When using Azure SQL Database, externally encrypted records cannot be queried using T-SQL (other than “retrieve all”) and may require a schema change such as the introduction of surrogate keys to enable retrieval of specific records or ranges of records.
EKM-03.2: Encryption & Key Management - Sensitive Data Protection	*Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?*	Y			Customers may configure Azure to enable encryption-in-transit by configuring HTTPS endpoints. Customers using Virtual Machines who wish to encrypt traffic between Web clients and Web servers in their VMs can implement TLS. Other enhancements to network traffic security include using IPsec VPNs or ExpressRoute to encrypt direct communications between the customer’s datacenter and Microsoft Azure. For Azure SQL Database, all communication to and from SQL Database requires encryption (TLS 1.1) at all times. For customers who are connecting with a client that does not validate certificates upon connection, the connection to SQL Database is susceptible to "man in the middle" attacks. It is the customer’s responsibility to determine if they are susceptible to this type of attack. Certificates must use a minimum of 2048-bit encryption.

EKM-03.3: Encryption & Key Management - Sensitive Data Protection	*Do you support tenant-generated encryption keys or permit tenants to encrypt data to an identity without access to a public key certificate (e.g., identity-based encryption)?*	Y			Azure supports the import of tenant-generated encryption keys through Azure Key Vault and may be performed through the Management Portal and programmatically via SMAPI
EKM-03.4: Encryption & Key Management - Sensitive Data Protection	*Do you have documentation establishing and defining your encryption management policies, procedures and guidelines?*	Y			Azure has documented and communicated Standard Operating Procedures (SOPs) that provide implementation guidance to operational teams. The SOPs provide documentation establishing and defining Azure encryption management policies, procedures and guidelines, are published at designated internal locations, and are reviewed annually. Cryptographic controls are used for information protection within the Microsoft Azure platform based on the Microsoft Azure Cryptographic Policy and Key Management procedures. Additional information may be obtained through the Customer's Account Manager.
EKM-04.1: Encryption & Key Management - Storage and Access	*Do you have platform and data appropriate encryption that uses open / validated formats and standard algorithms?*	Y			Azure supports strong cryptography using standard, validated formats including AES-256, IPSec, 1024-bit Perfect Forward Secrecy (PFS) and FIPS-140-2. Azure allows a customer to manage their own keys using independent Azure services for key vaulting, off-cloud third party key vaulting, or their own off-premises key management solution. Using Azure Key Vault, tenants can encrypt keys and secrets (such as authentication keys, storage account keys, data encryption keys, .PFX files, and passwords) by using keys that are protected by hardware security modules (HSMs). For added assurance, customers can import or generate keys in HSMs (keys never leave the HSM boundary). HSMs are certified to FIPS 140-2 level 2.
EKM-04.2: Encryption & Key Management - Storage and Access	*Are your encryption keys maintained by the cloud consumer or a trusted key management provider?*	Y			Azure supports both topologies.
EKM-04.3: Encryption & Key Management - Storage and Access	*Do you store encryption keys in the cloud?*	Y			For customers, Azure Key Vault enables users to store and use cryptographic keys within the Microsoft Azure environment. Azure Key Vault supports multiple key types and algorithms and enables the use of Hardware Security Modules (HSM) for high value customer keys. Microsoft Azure uses Microsoft's corporate PKI infrastructure

					which functions as the CA, Registration Authority, and provides directory services to manage keys and certificates. The PKI service is used to generate SSL certificates for client-server communications as an infrastructure identity. All SSL certificates are issued directly by Microsoft via SSLAdmin and have a 2048-bit key size with validity for two years.
EKM-04.4: Encryption & Key Management - Storage and Access	*Do you have separate key management and key usage duties?*	Y			Azure has established and implemented procedures to enforce segregation of key management and key usage duties. Azure key management encompasses the entire life cycle of cryptographic keys and has identified a method for establishing and managing keys in each management phase from generation, installation, storage, rotation and destruction.

Governance and Risk Management: Controls GRM-01 through GRM-11

Control ID in CCM	Consensus Assessment Questions (CCM Version 3.0.1, Final)	Microsoft Azure Response			
		Yes	No	N/A	Notes
GRM-01.1: Governance and Risk Management - Baseline Requirements	*Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?*	Y			Microsoft Azure production servers are inspected prior to installation in the production environment to ensure they are configured in compliance with baseline security and operational settings appropriate to the server's intended role.
GRM-01.2: Governance and Risk Management - Baseline Requirements	*Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?*	Y			Microsoft Azure has established baseline configuration standards and procedures are implemented to monitor for compliance against these baseline configuration standards.
GRM-01.3: Governance and Risk Management - Baseline Requirements	*Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?*	Y			Customers may create and upload a virtual hard disk (VHD) for use as their own image to create virtual machines in Azure.
GRM-02.1: Governance and Risk Management - Data Focus Risk Assessments	*Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status)?*	Y			Microsoft Azure performs an annual risk assessment that covers security, continuity, and operational risks. As part of this process, threats to security are identified and the risk from these threats is formally assessed. Azure also provides the multiple logging and monitoring mechanisms for their VMs, including Windows events themselves, that can be enabled programmatically via the monitoring and diagnostics service. The Azure Security Center provides a central view of the security state of Azure resources, to help verify that the appropriate security controls are in place and configured correctly.

GRM-02.2: Governance and Risk Management - Data Focus Risk Assessments	*Do you conduct risk assessments associated with data governance requirements at least once a year?*	Y			Microsoft Azure performs an annual risk assessment. As part of the overall ISMS framework baseline security requirements are constantly being reviewed, improved and implemented. Microsoft 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 the audit reports we have identified on the Azure website at: https://www.microsoft.com/en-us/TrustCenter/Compliance/default.aspx
GRM-03.1: Governance and Risk Management - Management Oversight	*Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?*	Y			Each management-endorsed version of the Information Security Policy and all subsequent updates are distributed to all relevant stakeholders. The Information Security Policy is made available to all new and existing Staff for review. All Microsoft Azure Staff represent that they have reviewed, and agree to adhere to, all policies within the Policy documents. All Microsoft Azure Contractor Staff agree to adhere to the relevant policies within the Policy. Should one of these parties not have access to this policy for any reason, the supervising Microsoft agent is responsible for distributing the policy to them.
GRM-04.1: Governance and Risk Management - Management Program	*Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?*	Y			An overall ISMS for Microsoft Azure has been designed and implemented to address industry best practices around security and privacy. A customer facing version of the Information 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 Information Security Policy.
GRM-04.2: Governance and Risk Management - Management Program	*Do you review your Information Security Management Program (ISMP) least once a year?*	Y			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-05.1: Governance and Risk Management - Management Support / Involvement	*Do you ensure your providers adhere to your information security and privacy policies?*	Y			Each management-endorsed version of the Information Security Policy and all subsequent updates are distributed to all relevant stakeholders. The Information Security Policy is made available to all new and existing Microsoft Azure employees for review. Information roles and responsibilities are clearly defined and assigned, and management at all levels is responsible for ensuring policies are followed.

GRM-06.1: Governance and Risk Management - Policy	*Do your information security and privacy policies align with industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?*	Y			Microsoft Azure has designed and implemented an ISMS framework that addresses industry best-practices for information security and privacy, based on open standards including ISO 27001, NIST 800-53 / 37, PCI DSS, and others. The ISMS has been documented and communicated in a customer-facing Information 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. Microsoft Azure information security and privacy policies align with industry standards align with many industry standards and are described in the Azure Trust Center.
GRM-06.2: Governance and Risk Management - Policy	*Do you have agreements to ensure your providers adhere to your information security and privacy policies?*	Y			Yes. All Microsoft Azure Contractor Staff agree to adhere to the relevant policies within the Information Security Policy. Agreements are in place that specify security and privacy compliance requirements for all third party contractors. Contracting staff suspected of committing breaches of security and/or violations of the Information Security Policy are subject to formal investigation and action appropriate to the associated contract, which may include termination of such contracts.
GRM-06.3: Governance and Risk Management - Policy	*Can you provide evidence of due diligence mapping of your controls, architecture and processes to regulations and/or standards?*	Y			All compliance documents reference a standard and can be verified by this document and others on the Azure Trust Center website. A customer facing version of the Information 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 Information Security Policy.
GRM-06.4: Governance and Risk Management - Policy	*Do you disclose which controls, standards, certifications and/or regulations you comply with?*	Y			Microsoft Azure provides a listing of all controls, standards, certifications and/or regulations complied with, both in publicly disclosed information on the Azure website and through security documents shared with customers available under NDA.
GRM-07.1: Governance and Risk Management - Policy Enforcement	*Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?*	Y			Microsoft Azure services staff suspected of committing breaches of security and/or violating the Information 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 Information 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-07.2: Governance and Risk Management - Policy Enforcement	*Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?*	Y			All employees are required to read and acknowledge the policies which detail possible actions in the event of a violation.
GRM-08.1: Governance and Risk Management - Policy Impact on Risk Assessments	*Do risk assessment results include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective?*	Y			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 the management through a formal risk assessment report. Microsoft Azure Risk Management organization bases the risk assessment framework on the ISO27001 standards. An integrated part of the methodology is the risk assessment process. Decisions to update policies and procedures are based on the risk assessment reports. Risk assessments are regularly reviewed based on periodicity and changes emerging to the risk landscape.
GRM-09.1: Governance and Risk Management - Policy Reviews	*Do you notify your tenants when you make material changes to your information security and/or privacy policies?*	Y			In the event a significant change is required in the security requirements, it may be reviewed and updated outside of the regular schedule. Changes to security and privacy policies which impact tenants are formally communicated to the designated point of contact.
GRM-09.2: Governance and Risk Management - Policy Reviews	*Do you perform, at minimum, annual reviews to your privacy and security policies?*	Y			The Microsoft Azure Information Security Policy undergoes a formal management review and update process at a regularly scheduled interval not to exceed 1 year.
GRM-10.1: Governance and Risk Management - Risk Assessments	*Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all*	Y			Azure performs an annual risk assessment. As part of the overall ISMS framework baseline security requirements are constantly being reviewed, improved and implemented. Microsoft 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 the audit reports we have identified on the Azure website.

	identified risks, using qualitative and quantitative methods?				
GRM-10.2: Governance and Risk Management - Risk Assessments	*Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)?*	Y			The Risk Assessment Assess phase begins with identifying risks, establishing a risk level by determining the likelihood of occurrence and impact, and finally, identifying controls and safeguards that reduce the impact of the risk to an acceptable level. According measures, recommendations and controls are put in place to mitigate the risks to the extent possible.
GRM-11.1: Governance and Risk Management - Risk Management Framework	*Do you have a documented, organization-wide program in place to manage risk?*	Y			The Risk Assessment program is in place throughout the Microsoft Azure and Microsoft enterprise. 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.
GRM-11.2: Governance and Risk Management - Risk Management Framework	*Do you make available documentation of your organization-wide risk management program?*	Y			Risk management documentation is made available through the various published audit reports made available on the Azure Trust Center website.

Human Resources: Controls HRS-01 through HRS-11

Control ID in CCM	Consensus Assessment Questions (CCM Version 3.0.1, Final)	Microsoft Azure Response			
		Yes	No	N/A	Notes
HRS-01.1: Human Resources - Asset Returns	*Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?*	Y			Microsoft Corporate Human Resources Policy drives employee termination processes and in coordination with management, ensures all organizationally-owned assets are returned upon employee or contractor termination. 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-01.2: Human Resources - Asset Returns	*Is your Privacy Policy aligned with industry standards?*	Y			Microsoft Azure is first major cloud provider to adopt the ISO 27018 privacy standard. Privacy Policy aligns with relevant statutory, regulatory and contractual requirements identified by Microsoft. Azure operates under the following five principles: **Consent:** CSPs must not use the personal data they receive for advertising and marketing unless expressly instructed to do so by the customer. Moreover, it must be possible for a customer to use the service without submitting to such use of its personal data for advertising or marketing. **Control:** Customers have explicit control of how their information is used. **Transparency:** CSPs must inform customers where their data resides, disclose the use of subcontractors to process PII and make clear commitments about how that data is handled. Communication: In case of a breach, CSPs should notify customers, and keep clear records about the incident and the response to it. **Independent and yearly audit:** A successful third-party audit of a CSP's compliance documents the service's conformance with the standard, and can then be relied upon by the customer to support their own regulatory obligations. To remain compliant, the CSP must subject itself to yearly third-party reviews.
HRS-02.1: Human Resources - Background Screening	*Pursuant to local laws, regulations, ethics and contractual constraints, are all employment candidates,*	Y			Pursuant to local laws, regulations, ethics and contractual constraints, all 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.

	contractors and involved third parties subject to background verification?				
HRS-03.1: Human Resources - Employment Agreements	*Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?*	Y			All Microsoft Azure contractor staff and FTE staff are required to take any training determined to be appropriate, such as Microsoft Privacy 101, to the services being provided and the role they perform.
HRS-03.2: Human Resources - Employment Agreements	*Do you document employee acknowledgment of training they have completed?*	Y			All FTE and third-party training is tracked and verified.
HRS-03.3: Human Resources - Employment Agreements	*Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?*	Y			Microsoft Azure has established confidentiality and non-disclosure agreements for protection of customer information within its environment. Responsibilities are designated to validate that agreements include relevant confidentiality, privacy, and security requirements.
HRS-03.4: Human Resources - Employment Agreements	*Is successful and timed completion of the training program considered a prerequisite for acquiring and maintaining access to sensitive systems?*	Y			Successful completion of required security and privacy training is required for all FTE and contractors granted access to sensitive systems.
HRS-03.5: Human Resources - Employment Agreements	*Are personnel trained and provided with awareness programs at least once a year?*	Y			All Microsoft Azure, Microsoft FTE and contractors are required to complete security and privacy training upon hire and annually thereafter. Security Awareness training is also provided in an ongoing basis through a variety of media.

HRS-04.1: Human Resources - Employment Termination	*Are documented policies, procedures and guidelines in place to govern change in employment and / or termination?*	Y			Microsoft Corporate Human Resources Policy drives employee termination processes and Microsoft Policy clearly defined 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 all resources, both physical and electronic.
HRS-04.2: Human Resources - Employment Termination	*Do the above procedures and guidelines account for timely revocation of access and return of assets?*	Y			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 all resources, both physical and electronic.
HRS-05.1: Human Resources - Mobile Device Management	*Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?*	Y			Microsoft Azure teams and personnel are required to adhere to applicable policies, which do not permit mobile computing devices to access the production environment, unless those devices have been approved for use by Microsoft Azure Management. Mobile computing access points are required to adhere with the wireless device security requirements.
HRS-06.1: Human Resources - Non-Disclosure Agreements	*Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented and*	Y			Microsoft Legal and Human Resources maintain policies and procedures defining the implementation and execution of non-disclosure and confidentiality agreements. 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.

	reviewed at planned intervals?				
HRS-07.1: Human Resources - Roles / Responsibilities	*Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?*	Y			Tenant roles and responsibilities are clearly defined in Azure policies which are acknowledged by tenants when subscribing to the service. The Information 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 Information 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-08.1: Human Resources - Technology Acceptable Use	*Do you provide documentation regarding how you may or access tenant data and metadata?*	Y			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 at the reference sites.
HRS-08.2: Human Resources - Technology Acceptable Use	*Do you collect or create metadata about tenant data usage through inspection technologies (search engines, etc.)?*		N		No. Azure does not share customer data with its advertiser-supported services, nor is customer data mined for marketing or advertising. This policy is backed by our enterprise cloud service agreements and reaffirmed by Microsoft's adoption of the international code of practice for cloud privacy, ISO/IEC 27018.
HRS-08.3: Human Resources - Technology Acceptable Use	*Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?*			N / A	Not applicable. Microsoft does not inspect customer subscription data.
HRS-09.1: Human Resources - Training / Awareness	*Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy,*	Y			All appropriate Microsoft employees take part in a Microsoft Azure 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. Microsoft also has non-disclosure provisions in our employee contracts. All Microsoft Azure contractor staff and MCIO staff are required

	nationality, cloud delivery model segregation of duties implications and conflicts of interest) for all persons with access to tenant data?				to take any training determined to be appropriate to the services being provided and the role they perform.
HRS-09.2: Human Resources - Training / Awareness	*Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?*	Y			All data is designated with stewardship with assigned responsibilities defined, documented and communicated.
HRS-10.1: Human Resources - User Responsibility	*Are users made aware of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards and applicable regulatory requirements?*	Y			All Microsoft Azure personnel are made aware of their roles and responsibilities through the use of multiple methods including regular newsletters, posters, live and computer-based training, policies and internal meetings. 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-10.2: Human Resources - User Responsibility	*Are users made aware of their responsibilities for maintaining a safe and secure working environment?*	Y			Yes. See HRS-10.1
HRS-10.3: Human Resources - User Responsibility	*Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?*	Y			Security policy defines requirements for secure operation of equipment, secure work areas, and policies regarding unattended equipment.
HRS-11.1: Human Resources - Workspace	*Do your data management policies and procedures address tenant and service*	Y			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 a MCIO host to one. Network connections are terminated after

	level conflicts of interests?				a defined period of inactivity. Conflict of interest definitions and FTE requirements are communicated and acknowledged by staff upon hire and at least annually thereafter.
HRS-11.2: Human Resources - Workspace	*Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to tenant data?*	Y			Hardware and software integrity monitoring are in place and audited on a regular basis.
HRS-11.3: Human Resources - Workspace	*Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build / configuration of the virtual machine?*	Y			The Microsoft Azure platform provides automated logging and alerting capabilities for monitoring system use and detection of potential unauthorized activity.

Identity and Access Management: Controls IAM-01 through IAM-13

Control ID in CCM	Consensus Assessment Questions (CCM Version 3.0.1, Final)	Microsoft Azure Response			
		Yes	No	N/A	Notes
IAM-01.1: Identity & Access Management - Audit Tools Access	*Do you restrict, log and monitor access to your information security management systems? (E.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)*	Y			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, CloudNet, Fabric, etc.) are configured to log and collect security events.
IAM-01.2: Identity & Access Management - Audit Tools Access	*Do you monitor and log privileged access (administrator level) to information security management systems?*	Y			Per IAM-01.2, all access to log and monitor systems is monitored and audited.
IAM-02.1: Identity & Access Management - Credential Lifecycle / Provision Management	*Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?*	Y			Access control policy is a component of overall policies and undergoes a formal review and update process. Access to Microsoft Azures' 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; all access is set to auto-expire on a preconfigured limit. • 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. Password policies for corporate domain accounts are managed through Microsoft corporate Active Directory policy that specifies minimum requirements for password length, complexity and expiry. The temporary passwords are communicated to the users using MSIT established processes. All services and infrastructure must at a minimum meet MSIT requirements but an internal organization can increase the

					strength past this standard, on their own discretion and to meet their security needs. It is the customer's responsibility to manage access to the Account Admin, Service Admin and Co-Admin roles within the Microsoft Azure portal.
IAM-02.2: Identity & Access Management - Credential Lifecycle / Provision Management	*Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?*	Y			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.
IAM-03.1: Identity & Access Management - Diagnostic / Configuration Ports Access	*Do you use dedicated secure networks to provide management access to your cloud service infrastructure?*	Yes			Microsoft Azure controls physical access to diagnostic and configuration ports through physical data center controls. Diagnostic and configuration ports are only accessible by arrangement between service/asset owner and hardware/software support personnel requiring access, using recommended secure administration workstations. Ports, services, and similar facilities installed on a computer or network facility, which are not specifically required for business functionality, are disabled or removed. 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.
IAM-04.1: Identity & Access Management - Policies and Procedures	*Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?*	Yes			Access control policy is a component of overall policies and undergoes a formal review and update process. Access to Microsoft Azures' 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 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-04.2: Identity & Access Management - Policies and Procedures	*Do you manage and store the user identity of all personnel who have network access, including their level of access?*	Y			See IAM-04.1
IAM-05.1: Identity & Access Management - Segregation of Duties	*Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?*	Y			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-06.1: Identity & Access Management - Source Code Access Restriction	*Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?*	Y			Microsoft Azure source code libraries are limited to authorized personnel. 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.
IAM-06.2: Identity & Access Management - Source Code Access Restriction	*Are controls in place to prevent unauthorized access to tenant application, program or object source code, and assure it is restricted to*	Y			Multiple physical, technical and logical controls are in place and monitored to prevent unauthorized access to restricted data.

	authorized personnel only?				
IAM-07.1: Identity & Access Management - Third Party Access	*Do you provide multi-failure disaster recovery capability?*	Y			Identification of risks related to external parties and access controls is performed as part of our Risk Management program and verified as part of our ISO 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 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.
IAM-07.2: Identity & Access Management - Third Party Access	*Do you monitor service continuity with upstream providers in the event of provider failure?*	Y			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.
IAM-07.3: Identity & Access Management - Third Party Access	*Do you have more than one provider for each service you depend on?*	Y			Based on risk and criticality, multiple service providers are engaged.
IAM-07.4: Identity & Access Management - Third Party Access	*Do you provide access to operational redundancy and continuity summaries, including the services you depend on?*	Y			Operation redundancy is in place for dependent services. Additional risks related to granting access to facilities and information systems are controlled and managed by MSIT.
IAM-07.5: Identity & Access Management - Third Party Access	*Do you provide the tenant the ability to declare a disaster?*	Y			Tenants may independently declare a disaster.

IAM-07.6: Identity & Access Management - Third Party Access	*Do you provide a tenant-triggered failover option?*	Y			Tenants may initiate failover mechanisms at their discretion.
IAM-07.7: Identity & Access Management - Third Party Access	*Do you share your business continuity and redundancy plans with your tenants?*		N		BCPs are documented and reviewed annually, and are attested by external auditors conducting compliance reviews for ISO, SOC, PCI, FedRAMP, and other standards.
IAM-08.1: Identity & Access Management - Trusted Sources	*Do you document how you grant and approve access to tenant data?*	Y			When granted, access is carefully controlled and logged. Strong authentication, including the use of multi-factor authentication, helps limit access to authorized personnel only. Access is revoked as soon as it is no longer needed. 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-08.2: Identity & Access Management - Trusted Sources	*Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?*		N		No. Data classification methodologies are not integrated, however, Azure platform data classification is designed to ensure tenant data classification policies are enforced when implemented.
IAM-09.1: Identity & Access Management - User Access Authorization	*Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners and/or*	Y			Microsoft Azure has adopted applicable corporate and organizational security policies, including an Information Security Policy. The policies have been approved, published and communicated to Microsoft Azure personnel. The Information Security Policy requires that access to Microsoft Azure assets to 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

	suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?				authorization, removal of access rights and periodic access reviews.
IAM-09.2: Identity & Access Management - User Access Authorization	*Do you provide upon request user access (e.g., employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?*	Y			Where approved and authorized according to the Azure ISMS, user access to data or assets is granted.
IAM-10.1: Identity & Access Management - User Access Reviews	*Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?*	Y			The Information Security Policy requires that access to Microsoft Azure assets to 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. Privileged accounts are reviewed at least every three (3) months to ensure the privileged access level is still appropriate. Access is modified based on the results of the reviews. A quarterly review is performed by FTE managers to validate the appropriateness of access to MCIO-managed network devices. A quarterly review is performed by FTE managers and MCIO security group owners to validate the appropriateness of user access. Security group memberships are reviewed for appropriateness on a quarterly basis and access is modified based on the results of the review.

IAM-10.2: Identity & Access Management - User Access Reviews	*If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?*	Y			Procedures have been established to disable access for terminated or transferred users within 5 business days.
IAM-10.3: Identity & Access Management - User Access Reviews	*Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data?*	Y			If tenant data was inappropriately accessed, tenants will be notified. Entitlement remediation and certification reports may be shared on a case by case basis.
IAM-11.1: Identity & Access Management - User Access Revocation	*Is timely deprovisioning, revocation or modification of user access to the organizations systems, information assets and data implemented upon any change in status of employees, contractors, customers, business partners or involved third parties?*	Y			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. Within the Microsoft Azure environment, customers are responsible for managing access to the applications customers host on Microsoft Azure.
IAM-11.2: Identity & Access Management - User Access Revocation	*Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?*	Y			Access permissions are reviewed and modified as appropriate during both a change in role or termination.

IAM-12.1: Identity & Access Management - User ID Credentials	*Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?*	Y			Password policies for corporate domain accounts are managed through Microsoft corporate Active Directory policy that specifies minimum requirements for password length, complexity and expiry. The temporary passwords are communicated to the users using MSIT established processes. All services and infrastructure must at a minimum meet MSIT 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-12.2: Identity & Access Management - User ID Credentials	*Do you use open standards to delegate authentication capabilities to your tenants?*	Y			Standards including SMAPI and REST APIs are supported.
IAM-12.3: Identity & Access Management - User ID Credentials	*Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?*	Y			Currently customers can manage their subscription by connecting to the Azure Management Portal over "https" or programmatically via REST API with their unique federated identity (customer domain AD user name and password). This grants the authenticated user with access to the connection string and administrator login and password for that particular Azure Subscription. Azure supports OpenID Connect, OAuth 2.0, and WS-Federation.
IAM-12.4: Identity & Access Management - User ID Credentials	*Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?*		N		Customers may control access using IP policies to prevent logins from certain regions.
IAM-12.5: Identity & Access Management - User ID Credentials	*Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?*	Y			Azure AD provides identity management and RBAC capabilities, but customers must configure policies and entitlements as dictated by their business needs.

IAM-12.6: Identity & Access Management - User ID Credentials	*Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, biometrics, etc.) for user access?*	Y			Azure Multi-Factor Authentication helps safeguard access to data and applications, and delivers strong authentication with a range of easy verification options—phone call, text message, or mobile app notification—allowing users to choose the method they prefer. https://azure.microsoft.com/en-us/services/multi-factor-authentication/
IAM-12.7: Identity & Access Management - User ID Credentials	*Do you allow tenants to use third-party identity assurance services?*	Y			Customers may implement third party assurance solutions.
IAM-12.8: Identity & Access Management - User ID Credentials	*Do you support password (minimum length, age, history, complexity) and account lockout (lockout threshold, lockout duration) policy enforcement?*	Y			The creation and allocation of passwords and PINs are managed through the standard account management processes. Policies and standards have been established and implemented for password expiration, length, complexity and history.
IAM-12.9: Identity & Access Management - User ID Credentials	*Do you allow tenants/customers to define password and account lockout policies for their accounts?*	Y			Customers are responsible for configuring unsuccessful login settings for access via their enablers by: a. Enforcing a limit of 3 consecutive invalid access attempts by a user during a 15-minute interval; and b. Automatically locking the account for 30 minutes, locking the account until it is released by an administrator, or delaying the next login prompt for the organization's defined delay when the maximum number of unsuccessful attempts is exceeded.
IAM-12.10: Identity & Access Management - User ID Credentials	*Do you support the ability to force password changes upon first logon?*	Y			The customer sets the password for the Azure portal root account at time of account creation.
IAM-12.11: Identity & Access Management - User ID Credentials	*Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge*	Y			Microsoft Azure Active Directory password policy requirements are enforced on the new passwords supplied by customers within the AADUX portal. Customer initiated self-service password changes require validation of older password. Administrator reset passwords are required to be changed upon subsequent login.

	questions, manual unlock)?				
IAM-13.1: Identity & Access Management - Utility Programs Access	*Are utilities that can significantly manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted and monitored?*	Y			Utility programs undergo changes and the release management process and are restricted to authorized personnel only. Administrative access and privileges to the Azure 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.
IAM-13.2: Identity & Access Management - Utility Programs Access	*Do you have a capability to detect attacks that target the virtual infrastructure directly (e.g., shimming, Blue Pill, Hyper jumping, etc.)?*	Y			A variety of software and hardware based technical controls are in place to detect attacks directed at Azure virtual infrastructure.
IAM-13.3: Identity & Access Management - Utility Programs Access	*Are attacks that target the virtual infrastructure prevented with technical controls?*	Y			A variety of technical controls are in place to prevent attacks including, but not limited to, Next-Generation firewalls, IDS/APS, network segmentation and network security analytics.

Infrastructure and Virtualization Security: Controls IVS-01 through IVS-13

Control ID in CCM	Consensus Assessment Questions (CCM Version 3.0.1, Final)	Microsoft Azure Response			
		Yes	No	N/A	Notes
IVS-01.1: Infrastructure & Virtualization Security - Audit Logging / Intrusion Detection	*Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents?*	Y			Forefront Identity Manager and IDS tools are implemented within the Azure environment. Microsoft Azure uses and Early Warning System (EWS) to support real-time analysis of events within its operational environment. Monitoring Agents and the Azure Incident Management System generate near real-time alerts about events that could potentially compromise the system.
IVS-01.2: Infrastructure & Virtualization Security - Audit Logging / Intrusion Detection	*Is physical and logical user access to audit logs restricted to authorized personnel?*	Y			MCIO restricts access to audit logs to authorized personnel based on job responsibilities. Event logs are archived on OSSC's secure archival infrastructure and are retained for 180 days.
IVS-01.3: Infrastructure & Virtualization Security - Audit Logging / Intrusion Detection	*Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done?*	Y			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 OSSC's secure archival infrastructure and are retained for 180 days. "Audit logging" is covered under the ISO 27001 standards and additional details can be found in the audit reports provided on the Azure Trust Center website.
IVS-01.4: Infrastructure & Virtualization Security - Audit Logging / Intrusion Detection	*Are audit logs centrally stored and retained?*	Y			Logging of service, user and security events (web server logs, FTP server logs, etc.) is enabled and retained centrally.
IVS-01.5: Infrastructure & Virtualization Security - Audit Logging / Intrusion Detection	*Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?*	Y			MCIO-managed network devices are configured to log and collect security events. The list of auditable events is reviewed and updated periodically or whenever there is a change in the systems' threat environment. MCIO has established monitoring systems to detect audit processing failures and report to appropriate personnel. Audit logs are stored for a minimum of 180 days.

IVS-02.1: Infrastructure & Virtualization Security - Change Detection	*Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)?*	Y			Read and write operations to virtual machines are logged via storage analytics, which the customer can view within their own storage account. Azure Virtual Machines staged in the Azure Gallery are maintained according to established software asset management procedures, which includes update logs to stored VHDs.
IVS-02.2: Infrastructure & Virtualization Security - Change Detection	*Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g., portals or alerts)?*	Y			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 their VMs automatically. Otherwise, customers have the option to upgrade to the latest OS image through the portal. In case of a VM role, customers are responsible for evaluating and updating their VMs.
IVS-03.1: Infrastructure & Virtualization Security - Clock Synchronization	*Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?*	Y			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-04.1: Infrastructure & Virtualization Security - Information System Documentation	*Do you provide documentation regarding what levels of system (network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances / scenarios?*	Y			The following operational processes 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. 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. Customers are responsible for monitoring and planning the capacity needs of their applications.
IVS-04.2: Infrastructure & Virtualization	*Do you restrict use of the memory oversubscription*	Y			Customer VMs are prevented from oversubscribing memory resources by the Azure hypervisor, which only allocates as much memory as has been requested by the VM when it is

Security - Information System Documentation	*capabilities present in the hypervisor?*				instantiated. Azure does not allow VMs to write to more memory than is initially allocated.
IVS-04.3: Infrastructure & Virtualization Security - Information System Documentation	*Do your system capacity requirements take into account current, projected and anticipated capacity needs for all systems used to provide services to the tenants?*	Y			Microsoft Azure Capacity Management team projects future capacity requirements based on internal operational reports, revenue forecasts and inputs from internal component teams.
IVS-04.4: Infrastructure & Virtualization Security - Information System Documentation	*Is system performance monitored and tuned in order to continuously meet regulatory, contractual and business requirements for all the systems used to provide services to the tenants?*	Y			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.
IVS-05.1: Infrastructure & Virtualization Security - Vulnerability Management	*Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?*	Y			Vulnerability assessment and scanning tools are specifically designed to operate in virtualized environments. Procedures have been established and implemented to scan for vulnerabilities on MCIO-managed hosts in the scope boundary. MCIO implements vulnerability scanning on server operating systems, databases, and network devices. The 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. Red-Team exercises are also routinely performed and results used to make security improvements.
IVS-06.1: Infrastructure & Virtualization Security - Network Security	*For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?*	Y			SQL Azure employs boundary protection devices such as SQL Azure Gateways, CGs, application firewalls and DOSGuard to control communications at external and internal boundaries. 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. Security best practices and guidance on defense in depth are published on the Azure website.

IVS-06.2: Infrastructure & Virtualization Security - Network Security	*Do you regularly update network architecture diagrams that include data flows between security domains/zones?*	Y			Yes. Internal diagrams are updated at least annually or as changes are made to the network.
IVS-06.3: Infrastructure & Virtualization Security - Network Security	*Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?*	Y			Yes. All firewall rules and ACLs are documented and reviewed on at least a quarterly basis. All 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-06.4: Infrastructure & Virtualization Security - Network Security	*Are all firewall access control lists documented with business justification?*	Y			Yes. All firewall rules and ACLs are documented and reviewed on at least a quarterly basis. All changes are required to follow the approved firewall rule change control process.
IVS-07.1: Infrastructure & Virtualization Security - OS Hardening and Base Controls	*Are operating systems hardened to provide only the necessary ports, protocols and services to meet business needs using technical controls (i.e. antivirus, file integrity monitoring and logging) as part of their baseline build standard or template?*		N		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. Azure Anti-Malware Services are available on Azure Gallery OS images by default, but must be enabled by the customer.
IVS-08.1: Infrastructure & Virtualization Security - Production / Non-Production Environments	*For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?*	Y			Within the Azure platform, tenants define their own production and non-production environments. For the Azure infrastructure, production and non-production are physically and logically separated. Microsoft Azure employs network-based and host-based boundary protection devices such as firewalls, load balancers, IPFilters, jumpboxes and front-end components. These devices use mechanisms such as VLAN isolation, NAT and packet filtering to separate customer traffic from management traffic. 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.
IVS-08.2: Infrastructure & Virtualization Security - Production / Non-Production Environments	*For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?*	Y			Azure provides guidance on configuring multiple environments through web documentation, blogs, TechNet, diagrams, Video on Demand and through Azure web-based training.
IVS-08.3: Infrastructure & Virtualization Security - Production / Non-Production Environments	*Do you logically and physically segregate production and non-production environments?*	Y			For the Azure infrastructure, production and non-production are physically and logically separated. Microsoft Azure employs network-based and host-based boundary protection devices such as firewalls, load balancers, IPFilters, jumpboxes and front-end components. These devices use mechanisms such as VLAN isolation, NAT and packet filtering to separate customer traffic from management traffic. 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.
IVS-09.1: Infrastructure & Virtualization Security - Segmentation	*Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?*	Y			Azure employs a defense in depth strategy for boundary protection, including secure segmentation of network environments through several methods including VLAN segmentation, ACL restrictions and encrypted communications for remote connectivity.
IVS-09.2: Infrastructure & Virtualization Security - Segmentation	*Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legislative, regulatory and contractual requirements?*	Y			Yes. System and network environments are isolated from each other using multiple technical controls.

IVS-09.3: Infrastructure & Virtualization Security - Segmentation	*Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?*	Y			For the Azure infrastructure, production and non-production are physically and logically separated. Microsoft Azure employs network-based and host-based boundary protection devices such as firewalls, load balancers, IPFilters, jumpboxes and front-end components. These devices use mechanisms such as VLAN isolation, NAT and packet filtering to separate customer traffic from management traffic.
IVS-09.4: Infrastructure & Virtualization Security - Segmentation	*Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?*	Y			Logical segregation is implemented to restrict unauthorized customer access to files / directories of other customers.
IVS-10.1: Infrastructure & Virtualization Security - VM Security	*Are secured and encrypted communication channels used when migrating physical servers, applications or data to virtual servers?*	Yes			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-10.2: Infrastructure & Virtualization Security - VM Security	*Do you use a network segregated from production-level networks when migrating physical servers, applications or data to virtual servers?*			N/A	Microsoft does not provide physical server migration.
IVS-11.1: Infrastructure & Virtualization Security - Hypervisor Hardening	*Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and*	Y			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. All management access requires multi-factor authentication, and all access is logged.

	supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?				
IVS-12.1: Infrastructure & Virtualization Security - Wireless Security	*Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?*	Y			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.
IVS-12.2: Infrastructure & Virtualization Security - Wireless Security	*Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings? (e.g., encryption keys, passwords, SNMP community strings)*			N / A	Wireless access to the Azure Production environment is not permitted. Wireless connections to Microsoft's corporate network must follow MSIT requirements for system health, security configuration, and policy enforcement.
IVS-12.3: Infrastructure & Virtualization Security - Wireless Security	*Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized*	Y			Privileges to MCIO systems and network devices are assigned to personnel based on least privilege principles in accordance with job responsibilities. Access to privileges is restricted through security groups.

	(rogue) network devices for a timely disconnect from the network?				
IVS-13.1: Infrastructure & Virtualization Security - Network Architecture	*Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?*	Y			Internal Azure diagrams clearly define boundaries and data flows between zones having different data classification, trust levels or compliance and regulatory requirements.
IVS-13.2: Infrastructure & Virtualization Security - Network Architecture	*Do you implement technical measures and 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?*	Y			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 (DDoS) attacks.

Interoperability and Portability: Controls IPY-01 through IPY-05

Control ID in CCM	Consensus Assessment Questions (CCM Version 3.0.1, Final)	Microsoft Azure Response			
		Yes	No	N/A	Notes
IPY-01.1: Interoperability & Portability - APIs	*Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?*	Y			A full set of Windows PowerShell cmdlets for the Azure API Management API is available via the standard Azure PowerShell installer.
IPY-02.1: Interoperability & Portability - Data Request	*Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?*	Y			Azure customers maintain access to their unstructured data stored with Azure and is available upon demand.
IPY-03.1: Interoperability & Portability - Policy & Legal	*Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?*	Y			Microsoft Azure has established designated responsibilities to review and execute service specific agreements and security requirements with third party service providers. Exchange of information between Microsoft Azure and third parties is governed through Information Exchange Agreements.
IPY-03.2: Interoperability & Portability - Policy & Legal	*Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?*	Y			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-04.1: Interoperability & Portability - Standardized	*Can data import, data export and service management be conducted over secure (e.g., non-*	Y			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).

Network Protocols	*clear text and authenticated), industry accepted standardized network protocols?*				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-04.2: Interoperability & Portability - Standardized Network Protocols	*Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?*	Y			MCIO configures information systems to provide only essential capabilities and specifically prohibits or restricts the use of the functions, ports, protocols, and/or services as per GSA, NIST, CIS guidelines, or industry best practices.
IPY-05.1: Interoperability & Portability - Virtualization	*Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g.., OVF) to help ensure interoperability?*	Y			Microsoft Azure supports virtualization industry standards including the OVF format.
IPY-05.2: Interoperability & Portability - Virtualization	*Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?*	Y			All available custom hooks are documented

Mobile Security: Controls MOS-01 through MOS-20

Control ID in CCM	Consensus Assessment Questions (CCM Version 3.0.1, Final)	Microsoft Azure Response			
		Yes	No	N/A	Notes
MOS-01.1: Mobile Security - Anti-Malware	*Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-02.1: Mobile Security - Application Stores	*Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-03.1: Mobile Security - Approved Applications	*Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores be loaded onto a mobile device?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-04.1: Mobile Security - Approved Software for BYOD	*Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.

MOS-05.1: Mobile Security - Awareness and Training	*Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-06.1: Mobile Security - Cloud Based Services	*Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-07.1: Mobile Security - Compatibility	*Do you have a documented application validation process for testing device, operating system and application compatibility issues?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-08.1: Mobile Security - Device Eligibility	*Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-09.1: Mobile Security - Device Inventory	*Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (os system and patch levels, lost or decommissioned, device assignee)?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.

MOS-10.1: Mobile Security - Device Management	*Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-11.1: Mobile Security - Encryption	*Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-12.1: Mobile Security - Jailbreaking and Rooting	*Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-12.2: Mobile Security - Jailbreaking and Rooting	*Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.

MOS-13.1: Mobile Security - Legal	*Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery and legal holds?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-13.2: Mobile Security - Legal	*Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-14: Mobile Security - Lockout Screen	*Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-15: Mobile Security - Operating Systems	*Do you manage all changes to mobile device operating systems, patch levels and applications via your company's change management processes?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-16.1: Mobile Security - Passwords	*Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.

MOS-16.2: Mobile Security - Passwords	*Are your password policies enforced through technical controls (i.e. MDM)?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-16.3: Mobile Security - Passwords	*Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-17.1: Mobile Security - Policy	*Do you have a policy that requires BYOD users to perform backups of specified corporate data?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-17.2: Mobile Security - Policy	*Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-17.3: Mobile Security - Policy	*Do you have a policy that requires BYOD users to use anti-malware software (where supported)?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-18.1: Mobile Security - Remote Wipe	*Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-18.2: Mobile Security - Remote Wipe	*Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.

MOS-19.1: Mobile Security - Security Patches	*Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-19.2: Mobile Security - Security Patches	*Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-20.1: Mobile Security - Users	*Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-20.2: Mobile Security - Users	*Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.

Security Incident Management, E-Discovery & Cloud Forensics: Controls SEF-01 through SEF-05

Control ID in CCM	Consensus Assessment Questions (CCM Version 3.0.1, Final)	Microsoft Azure Response			
		Yes	No	N/A	Notes
SEF-01.1: Security Incident Management, E-Discovery & Cloud Forensics - Contact / Authority Maintenance	*Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?*	Y			Microsoft Azure has designated responsibilities and established processes to maintain contacts with external authorities across all jurisdictions in which it operates. 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.
SEF-02.1: Security Incident Management, E-Discovery & Cloud Forensics - Incident Management	*Do you have a documented security incident response plan?*	Y			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 Microsoft Azure Incident Response process follows the following 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 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-02.2: Security Incident Management, E-Discovery & Cloud Forensics - Incident Management	*Do you integrate customized tenant requirements into your security incident response plans?*	Y			In the event a tenant is impacted by an event, Azure has clearly defined incident response plans and notification requirements.
SEF-02.3: Security Incident Management, E-Discovery & Cloud Forensics - Incident Management	*Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?*	Y			Microsoft publishes information on Security Incident Notification as part of the Azure Online Services Terms available publicly here: http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=31. If Microsoft becomes aware of any unlawful access to any Customer Data stored on Microsoft's equipment or in Microsoft's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data (each a "Security Incident"), Microsoft will promptly (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; and (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident. Notification(s) of Security Incidents will be delivered to one or more of Customer's administrators by any means Microsoft selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on each applicable Online Services portal. Microsoft's obligation to report or respond to a Security Incident under this section is not an acknowledgement by Microsoft of any fault or liability with respect to the Security Incident. Customer must notify Microsoft promptly about any possible misuse of its accounts or authentication credentials or any security incident related to an Online Service.
SEF-02.4: Security Incident Management, E-Discovery & Cloud Forensics - Incident Management	*Have you tested your security incident response plans in the last year?*	Y			Security and incident response plans are continually updated and tested at least annually.
SEF-03.1: Security Incident Management, E-Discovery & Cloud Forensics	*Does your security information and event management (SIEM) system merge data*	Y			Azure Diagnostics are extensions that enable you to collect diagnostic telemetry data from a worker role, web role, or virtual machine running in Azure. The telemetry data is stored in an Azure storage account and can be used for debugging and troubleshooting, measuring performance, monitoring

- Incident Reporting	*sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?*				resource usage, traffic analysis and capacity planning, and auditing.
SEF-03.2: Security Incident Management, E-Discovery & Cloud Forensics - Incident Reporting	*Does your logging and monitoring framework allow isolation of an incident to specific tenants?*	Y			The Azure logging and monitoring infrastructure 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-04.1: Security Incident Management, E-Discovery & Cloud Forensics - Incident Response Legal Preparation	*Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?*	Y			Security incident response plans and collection of evidence adheres to the ISO 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-04.2: Security Incident Management, E-Discovery & Cloud Forensics - Incident Response Legal Preparation	*Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?*	Y			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-04.3: Security Incident Management, E-Discovery & Cloud Forensics - Incident Response Legal Preparation	*Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?*	Y			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.
SEF-04.4: Security Incident Management, E-Discovery & Cloud Forensics - Incident Response Legal Preparation	*Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?*	Y			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-05.1: Security Incident Management, E-Discovery & Cloud Forensics - Incident Response Metrics	*Do you monitor and quantify the types, volumes and impacts on all information security incidents?*	Y			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.
SEF-05.2: Security Incident Management, E-Discovery & Cloud Forensics - Incident Response Metrics	*Will you share statistical information for security incident data with your tenants upon request?*	Y			Microsoft 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.

Supply Chain Management, Transparency and Accountability: Controls STA-01 through STA-09

Control ID in CCM	Consensus Assessment Questions (CCM Version 3.0.1, Final)	Microsoft Azure Response			
		Yes	No	N/A	Notes
STA-01.1: Supply Chain Management, Transparency and Accountability - Data Quality and Integrity	*Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?*	Y			Azure works with various business groups to protect against supply chain threats throughout the supply chain lifecycle. These groups support Azure in creating purchase orders, accelerating deliveries, performing quality checks, processing warranty claims and obtaining spares.
STA-01.2: Supply Chain Management, Transparency and Accountability - Data Quality and Integrity	*Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?*	Y			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-02.1: Supply Chain Management, Transparency and Accountability - Incident Reporting	*Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?*	Y			Microsoft 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-03.1: Supply Chain Management, Transparency and Accountability - Network / Infrastructure Services	*Do you collect capacity and use data for all relevant components of your cloud service offering?*	Y			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-03.2: Supply Chain Management, Transparency and Accountability - Network / Infrastructure Services	*Do you provide tenants with capacity planning and use reports?*	Y			Microsoft Azure Capacity Management team projects future capacity requirements based on internal operational reports, revenue forecasts and inputs from internal component teams. Customers may use the Azure Operational Insights dashboard to monitor and adjust their virtual environment according to their needs.
STA-04.1: Supply Chain Management, Transparency and Accountability - Provider Internal Assessments	*Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?*	Y			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 the 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-05.1: Supply Chain Management, Transparency and Accountability - Supply Chain Agreements	*Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored and transmitted?*	Y			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 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.
STA-05.2: Supply Chain Management, Transparency and Accountability - Supply Chain Agreements	*Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?*	Y			Microsoft requires that vendors comply with applicable laws, including data protection laws. Vendors must also sign on to Microsoft's EU Model Clauses, which requires compliance with EU data protection law.
STA-05.3: Supply Chain Management, Transparency and Accountability - Supply Chain Agreements	*Does legal counsel review all third-party agreements?*	Y			Microsoft requires all vendors to sign our agreements, which have had legal review; all third-party agreements involving access to customer data also go through legal review.

STA-05.4: Supply Chain Management, Transparency and Accountability - Supply Chain Agreements	*Do third-party agreements include provision for the security and protection of information and assets?*	Y			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, asset protection requirements and vendor access to relevant applications.
STA-05.5: Supply Chain Management, Transparency and Accountability - Supply Chain Agreements	*Do you provide the client with a list and copies of all sub-processing agreements and keep this updated?*	Y			Microsoft Azure provides a list of third party contractors on the Microsoft Trust Center: https://www.microsoft.com/en-us/TrustCenter/Privacy/default.aspx
STA-06.1: Supply Chain Management, Transparency and Accountability - Supply Chain Governance Reviews	*Do you review the risk management and governance processes of partners to account for risks inherited from other members of that partner's supply chain?*	Y			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 Microsoft CELA 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 CELA. Vendors requiring access to source code need to be approved by the GM and CELA, and sign a Source Code Licensing Agreement. 3. Additional risks related to granting access to facilities and information systems are controlled and managed by MSIT. Physical and network security for offsite vendor facilities are governed by MSIT.
STA-07.1: Supply Chain Management, Transparency and Accountability - Supply Chain Metrics	*Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate and relevant agreements (e.g., SLAs) between providers and customers (tenants)?*	Y			Microsoft Azure has established procedures and designated responsibilities for managing changes to third-party services. Microsoft Azure's designated teams manage third-party relationship 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.

STA-07.2: Supply Chain Management, Transparency and Accountability - Supply Chain Metrics	*Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?*	Y			Microsoft Azure has employed an independent assessor to develop a system assessment plan and conduct a controls assessment. Controls assessments are performed annually and the results are reported to relevant parties.
STA-07.3: Supply Chain Management, Transparency and Accountability - Supply Chain Metrics	*Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?*	Y			The services provided by third-party vendors are monitored against the service levels by designated responsibilities 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-07.4: Supply Chain Management, Transparency and Accountability - Supply Chain Metrics	*Do you review all agreements, policies and processes at least annually?*	Y			The services provided by third-party vendors are monitored against the service levels by designated responsibilities 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.
STA-08.1: Supply Chain Management, Transparency and Accountability - Third Party Assessment	*Do you assure reasonable information security across your information supply chain by performing an annual review?*	Y			Microsoft Azure contractually requires that its subcontractors meet important privacy and security requirements. Requirements and contracts are reviewed at least annually or as renewed. Microsoft Azure AD performs quarterly ISMS reviews.
STA-08.2: Supply Chain Management, Transparency and Accountability - Third Party Assessment	*Does your annual review include all partners/third-party providers upon which your information supply chain depends?*	Y			Microsoft Azure has employed an independent assessor to develop a system assessment plan and conduct a controls assessment. Controls assessments are performed annually and the results are reported to relevant parties.
STA-09.1: Supply Chain Management, Transparency and Accountability - Third Party Audits	*Do you permit tenants to perform independent vulnerability assessments?*	Y			For security and operational reasons, Microsoft Azure does not allow our customers to perform their own audits on Microsoft's Microsoft Azure platform service, although customers are allowed to perform non- invasive penetration testing of their own application with prior approval.

STA-09.2: Supply Chain Management, Transparency and Accountability - Third Party Audits	*Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?*	Y			Microsoft Azure contracts with independent assessors to perform penetration testing of the Microsoft Azure platform at least quarterly. Attestation to scans and their remediation can be found in the compliance and audit report documentation on the Azure website.

Threat and Vulnerability Management: Controls TVM-01 through TVM-03

Control ID in CCM	Consensus Assessment Questions (CCM Version 3.0.1, Final)	Microsoft Azure Response			
		Yes	No	N/A	Notes
TVM-01.1: Threat and Vulnerability Management - Anti-Virus / Malicious Software	*Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your systems?*	Y			The Microsoft Azure Security group responds to malicious events, including escalating and engaging specialized support groups. A number of key security parameters are monitored to identify potentially malicious activity on the systems. 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 all 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-01.2: Threat and Vulnerability Management - Anti-Virus / Malicious Software	*Do you ensure that security threat detection systems using signatures, lists or behavioral patterns are updated across all infrastructure components within industry accepted time frames?*	Y			Weekly and real-time scans are performed and alerts are generated to MOC upon detection of malicious code.
TVM-02.1: Threat and Vulnerability Management - Vulnerability / Patch Management	*Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?*	Y			Procedures have been established and implemented to scan for vulnerabilities on MCIO-managed hosts in the scope boundary. MCIO implements vulnerability scanning on server operating systems, databases, and network devices with appropriate vulnerability scanning tool. MCIO web applications are scanned with the appropriate scanning solution. The vulnerability scans are performed on a quarterly basis at 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 their VMs automatically. Otherwise, customers have the option to upgrade to the latest OS image through the portal. In

					case of a VM role, customers are responsible for evaluating and updating their VMs.
TVM-02.2: Threat and Vulnerability Management - Vulnerability / Patch Management	*Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?*	Y			Web applications are scanned with purpose-built, industry application security scanning tools.
TVM-02.3: Threat and Vulnerability Management - Vulnerability / Patch Management	*Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?*	Y			Vulnerability scans are performed at least quarterly. Microsoft Azure contracts with independent assessors to perform penetration testing of the Microsoft Azure boundaries.
TVM-02.4: Threat and Vulnerability Management - Vulnerability / Patch Management	*Will you make the results of vulnerability scans available to tenants at their request?*		N		Azure does not provide scans of customer VMs or any customer applications running on the VMs. Patching customer VMs is the responsibility of customers.
TVM-02.5: Threat and Vulnerability Management - Vulnerability / Patch Management	*Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications and systems?*	Y			A formal change control process is in place for testing, authorizing and promoting source code builds from pre-production environments to production based on defined entry/exit check-lists for each pre-production gate.
TVM-02.6: Threat and Vulnerability Management - Vulnerability / Patch Management	*Will you provide your risk-based systems patching time frames to your tenants upon request?*	Y			Microsoft 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.
TVM-03.1: Threat and Vulnerability Management - Mobile Code	*Is mobile code authorized before its installation and use, and the code configuration checked, to ensure*	Y			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 Microsoft Azure. The use of mobile code in the Microsoft Azure

	that the authorized mobile code operates according to a clearly defined security policy?				applications is reviewed during multiple phases of the SDL process.
TVM-03.2: Threat and Vulnerability Management - Mobile Code	*Is all unauthorized mobile code prevented from executing?*	Y			Multiple controls prevent unauthorized mobile code from executing.

2 References and Further Reading

The following resources are available to provide more general information about Microsoft Azure and related Microsoft services, as well as specific items referenced in the main text:

- Microsoft Azure Home – general information and links about Microsoft Azure
  - http://azure.microsoft.com
- Microsoft Azure Developer Center – developer guidance and information
  - http://msdn.microsoft.com/en-us/azure/default.aspx
- Security Best Practices For Developing Microsoft Azure Applications (white paper)
  - http://download.microsoft.com/download/7/3/E/73E4EE93-559F-4D0F-A6FC-7FEC5F1542D1/SecurityBestPracticesWindowsAzureApps.docx
- Microsoft's Security Development Lifecycle (SDL)
  - http://www.microsoft.com/security/sdl/
- Microsoft Cloud Infrastructure and Operations group
  - http://www.microsoft.com/en-us/server-cloud/cloud-os/global-datacenters.aspx
- Microsoft Security Response Center [where Microsoft security vulnerabilities, including issues with Microsoft Azure, can be reported]
  - http://www.microsoft.com/security/msrc/default.aspx
  - Or via email to secure@microsoft.com.
- Service Trust Portal
  - https://www.microsoft.com/en-us/TrustCenter/STP/default.aspx