

Microsoft Azure

Responses to Motion Picture Association of America Application and Cloud Security Guidelines

**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*

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

(c) 2016 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. Some examples are for illustration only and are fictitious. No real association is intended or inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

Table of Contents

[1 Introduction 4](#_Toc446076196)

[1.1 About This Document 4](#_Toc446076197)

[Microsoft Azure Responses to MPAA 2015 Application & Cloud Security Guidelines 6](#_Toc446076198)

[Application Security 6](#_Toc446076199)

[Cloud Security 26](#_Toc446076200)

[2 References and Further Reading 39](#_Toc446076201)

# Introduction

Content security and protection is critical for feature film development, as there are multiple points in the workflow where digital assets can be compromised or stolen. Dailies, rough cuts, and visual effects are just some of the materials exposed during normal production, and the box-office impacts of a security breach on a blockbuster project can reach tens of millions of dollars.

At the same time, production IT systems (in-house / on-premises or rented) remain a significant overhead expense for studios—one they would like to minimize while still protecting highly valuable content. By moving workflows into the Microsoft Azure public cloud, producers and content creators can enhance the security of their productions and:

* Offload the burdens of content protection and compliance to Azure;
* Take advantage of Microsoft’s decades of experience in security development, enterprise datacenters, and services;
* Use the scale and presence of Azure to enable global collaboration with ease;
* Burst high-demand traffic to the cloud for rendering, encoding, encryption, and more.

To help major studios, partners, and vendors design infrastructure and solutions that ensure the security of digital film assets, the [Motion Picture Association of America](http://www.mpaa.org/) (MPAA) provides best-practices guidance and security control frameworks. The MPAA also performs content security assessments on behalf of its member companies (Walt Disney Studios Motion Pictures, Paramount Pictures Corporation, Sony Pictures Entertainment Inc., Twentieth Century Fox Film Corporation, Universal City Studios LLC, and Warner Bros. Entertainment Inc.).

Microsoft Azure is the first hyper-scale, multi-tenant public cloud to successfully complete a security and compliance assessment by the MPAA’s independent auditors. This means that companies who do business with major studio film productions can use Azure to help reduce the IT costs normally associated with secure content creation, management, and distribution.

Azure complies with the MPAA’s best-practices guidelines for application and cloud security, covering the following services: Azure AD, ACS, Batch, Cache, CDN, ExpressRoute, Event Hubs (Service Bus), Import/Export Services, Media Services, Portal, Premium Storage, Scheduler, SQL DB, Storage, Storage Files, Virtual Machines, Virtual Networks, and WorkFlow.

## About This Document

While the [audit reports](mailto:contentsecurity@mpaa.org) are only distributed by the MPAA, the [guidelines are publicly available](http://www.mpaa.org/content-security-program/) (to go through an assessment, the service provider answers the questionnaires that detail the features, processes, and policies that ensure customer data security).

This “Application and Cloud Security Guidelines” document, and its companion “Azure Responses to MPAA Common Guidelines”, provide the framework for evaluating Azure’s capabilities to support secure content workflows in the cloud. The details presented below enable deep insight into core Azure operations and architecture, such as physical security, infrastructure management, privacy policies, business continuity, and more.

You will note that some responses are shaded blue. This indicates a question or control objective that is either the customer’s responsibility, or one that is distributed between the customer and Azure. For example, user data classification is up to the customer and how it defines security boundaries on content, but Azure also has system data that is classified according to Microsoft’s information security management policy. Azure provides features that customers can use to classify data, but does not itself classify a customer’s data within an Azure Storage account.

For more information about the MPAA frameworks and best-practices guidelines, please visit <http://www.mpaa.org/content-security-program/>.

Microsoft Azure Responses to MPAA 2015 Application & Cloud Security Guidelines

# Application Security

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Control IDs** | **MPAA Guidelines** | **Microsoft Azure Response** | | | |
| **Yes** | **No** | **N/A** | **Notes** |
| **Q. 100:**  AS-1.0 | *Do you use a system/software development methodology?* | X |  |  | Applies to: Rapid Application Development, Agile, other:  Microsoft Secure Development Lifecycle (SDL), Operational Security Assurance (OSA) |
| **Q. 101:**  AS-1.0 | *Do you perform a risk analysis for systems/software?* | X |  |  | Microsoft Azure's risk assessment approach was developed as part of Azure's ISO 27001 methodology and in accordance with the NIST 800-30 standard. In order to facilitate the risk assessment process, the following general steps were considered:   * Determine the extent of potential threat. * Identify which security controls in a system need to be applied. * Summarize residual risk. * Involve senior management to address specific actions taken or planned to correct deficiencies in security controls. * Reduce or eliminate known vulnerabilities in the information system.   The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30: Risk Management Guide for Information Technology (IT) Systems is leveraged to the extent possible in developing a risk assessment methodology for Microsoft Azure.  Vulnerabilities identified for the risk assessment were based on available NIST 800-30, NIST 800-53, and National Vulnerability database (U.S. government repository of standards-based vulnerability management data) guidance. |
| **Q. 102:**  AS-1.0 | *Do you utilize secure coding standards?* | X |  |  | Microsoft Secure Development Lifecycle, Operational Security Assurance  **Security Requirements Analysis and Specification**: Security requirements are identified during the planning phase and / or during the SDL review and captured in the specification document and/or bug log. SDL review is required for all Community Technology Preview (CTP) releases or at a minimum on a semi-annual basis. If threat modeling is required, threat models are documented, and unmitigated security threats are translated into security bugs to be resolved by the component teams.   **Secure Development Lifecycle**: Projects can fall into three (3) categories: SDL Full-serve, SDL Self-serve and SDL-optional. Results of the threat modeling review are translated into defects and are resolved prior to release. All portions of the SDL process must be completed and signed off. The SDL documentation such as threat models, code scan logs, and documentation around exceptions must be saved for audit purposes.   **Builds**: For all releases, virus scans of the stable builds are carried out prior to release into production. Virus scanning of OS builds are carried out by the Azure team. In addition, some releases go through fuzz testing (where applicable) based on the Azure Security Advisor’s recommendation and per the SDL requirements. Automated code analysis tools such as FxCop, BinScope and other tools are run as determined by the Security Advisor and the SDL requirements.   **Testing of Releases**: As part of the functional testing, the Component Test teams (or component team members acting in the equivalent role) test the builds in a test environment. Defects are created for bugs discovered. Security bugs created through the SDL process are also tested and resolved as part of the development process. Any open bugs are resolved prior to approval of the release. |
| **Q. 103:**  AS-1.0 | *Do you have change control process for migrating changes into production?* | X |  |  | The Change and Release Management process is used to plan, schedule, develop, approve, apply, distribute and track software changes to the production environment, through designated responsibilities. It further controls the integrity and reliability of the environment while maintaining the pace of changes required for business purposes.   Changes within the Microsoft Azure environment are divided into the following:   * **Software changes** – modification, enhancements and upgrades to the Microsoft Azure software * **Configuration changes** – configuration changes that do not require re-building of source code   The change management process includes the following:   * **Change Documentation** – Any and all changes to the production environment are documented and tracked through a central tracking system. * **Change Reviews** – The adherence to the established security, privacy and quality criteria are reviewed at defined intervals during the release process. A pre-acceptance review is performed on all changes prior to their acceptance in the release pipeline, which will lead to their release into production. Software builds are reviewed for their features as part of testing, security, and privacy checks, as part of the entry checklist criteria. Similarly, hardware and network changes have established validation steps to evaluate their adherence to the build requirements. * **Release reviews** – Releases are reviewed and authorized by individual Component Teams. Coordinated meetings consist of key members of different teams who need to synchronize their plans and releases due to dependencies. A Release Sign-off Record (RSR) is created to capture the sign-off from the key stakeholders including Component Team Manager, Live Site Management team, etc., involved in the release review. Changes to Microsoft Cloud Infrastructure and Operations (MCIO) managed network devices would include representation from the MCIO Global Networking Services (GNS) team. * **Change deployment** – Changes are deployed on scheduled intervals by the respective deployment teams. Release Mangers from the respective Component teams are responsible for the release review and signed-off prior to production deployment. The outcome of a change is monitored closely. Should the change result in a failure scenario the change is rolled-back to its previous state or a hotfix is deployed to address the failure. |
| **Q. 103A:**  AS-1.0 | *Do you have back out procedures in your change control process according to impact of change?* | X |  |  | Changes are deployed on scheduled intervals by the respective deployment teams. Release Managers from the respective Component teams are responsible for the release review and signed-off prior to production deployment. The outcome of a change is monitored closely. Should the change result in a failure scenario the change is rolled-back to its previous state or a hotfix is deployed to address the failure. |
| **Q. 103B:**  AS-1.0 | *Do you restrict to authorized persons the ability to promote changes into production environments?* | X |  |  | Segregation of duties is established on critical functions within the Microsoft Azure production environment, to minimize the risk of unauthorized changes to production systems.   Access to make changes to the production environment is limited to authorized team members. Temporary Just-in-Time (JIT) Access to the production environment by other teams (e.g. Component or Integration) may be granted for specific issue handling or troubleshooting purposes. JIT access is provisioned though the Azure Customer Information System (ACIS) portal based on the workflow configured. The access is short-lived and revoked per ACIS policy settings upon work completion. |
| **Q. 104:**  AS-1.0 | *Do you assign individual administrator accounts for each privileged user?* |  | X |  | Users are granted temporary JIT access based on their roles and responsibilities, using their existing Microsoft corporate Active Directory domain account. Roles include:   * **Submitter** (Component team members): Provides and tracks the releases through approved RSR after the predefined release entry criteria are met and after signoff from dependent teams (if required). * **Approver** (Component team Release Approvers): Approves RSR initiated by the submitter. * **Operator** (Component team): Manages Test/Production deployments, validates deployment scripts, validates the deployments and provides signoff. |
| **Q. 105:**  AS-1.0 | *Do you review user access on a quarterly basis?* | X |  |  | For user access rights to Microsoft Azure systems controlled through security groups created and managed by the internal identity tool, access is automatically terminated depending on the rules configured for the project. The user is required to resubmit a request for access when that individual’s access is expiring and will be re-adjudicated based on the defined rules.  User accounts (Identity Management Tool and local accounts) are reviewed and audited on a quarterly basis. The current user membership lists from the corresponding AD groups and tools are reviewed and users with access are verified. If any access is deemed inappropriate, an access removal request is initiated for access removal. |
| **Q. 106:**  AS-2.0 | *Do you track system accounts and who has access to them?* | X |  |  | Microsoft Azure leverages both the Microsoft Cloud Infrastructure and Operations (MCIO) and Microsoft Corporate Active Directory (AD) systems, managed by MCIO & Microsoft IT respectively to control access to key information systems. Microsoft Azure personnel are assigned unique corporate AD accounts by Microsoft IT as part of standard new employee on-boarding to Microsoft. All standard access requests and approvals are managed through the Identity Management Tool or Forefront Identity Manager, which are automated workflow management tools that track the process for account request, approval, creation, modification, and deletion.  See also the response to Question 105 above. |
| **Q. 106A:**  AS-1.0  AS-2.0 | *Do you change the passwords of system accounts periodically or when users (e.g., programmers, administrators, and contractors) no longer need access to them (e.g., project completion, termination)?* | X |  |  | Password policies for corporate domain accounts are managed through the Microsoft corporate AD policy that specifies minimum requirements for password length, complexity and expiry. Temporary passwords are communicated to the users using Microsoft IT established processes. Guidelines for password selection and use has been defined and published in Online Services Security Standards. |
| **Q. 107:**  AS-1.0 | *Do you restrict source code to authorized users?* | X |  |  | Changes to production environments go through the Change Management process. This process requires that:   * Pre-screened admin requests from Microsoft corporate networks are approved * That role based and Just-in-Time / Just Enough Access controls are enforced * Privileges issued are temporary and grant the least privilege required to complete tasks * Multi-factor authentication for administrative access is required * Access requests are logged and audited   Microsoft Azure source code libraries are limited to access by authorized personnel only. Where feasible, source code libraries maintain separate project work spaces for independent projects. Microsoft Azure and Microsoft Azure Contractors are granted access only to those work spaces to which they need access to perform their duties. Source code libraries enforce control over changes to source code by requiring a review from designated reviewers prior to submission. An audit log detailing modifications to the source code library is maintained. |
| **Q. 108:**  AS-1.0 | *Do you test applications prior to deployment?* | X |  |  | Software releases and configuration changes to the Azure platform are tested based on established criteria prior to production implementation, and procedures have been established to evaluate and implement Microsoft released patches to Azure infrastructure.  Customers have access to third party audit reports and certifications that encompass the controls relevant to change management. Customers also receive their roles, rights and responsibilities in the Azure Terms & Conditions. |
| **Q. 109:**  AS-1.0 | *Do you perform code review?* | X |  |  | Microsoft follows NIST guidance regarding security considerations in software development in that information security must be integrated into the SDLC from system inception. Continual integration of security practices in the Microsoft SDL enables early identification and mitigation of security vulnerabilities and misconfigurations; awareness of potential software coding challenges caused by required security controls; identification of shared security services and reuse of security best practices tools which improve security posture through proven methods and techniques; and enforces Microsoft's already comprehensive risk management program.   Microsoft Azure has established software development and release management processes to control implementation of major changes including:   * The identification and documentation of the planned change * Identification of business goals, priorities and scenarios during product planning * Specification of feature/component design * Operational readiness review based on a pre-defined criteria/check-list to assess overall risk/impact * Testing, authorization and change management based on entry/exit criteria for development, integration testing, pre-production, and production environments as appropriate.   MCIO uses standardized processes for the acquisition, preparation / provisioning, deployment, and configuration of physical assets such as compute servers, storage, and networking hardware. Security processes are in place to ensure supply chain integrity, including shipping / receiving from OEM partners, physical transfers, and installations in datacenter colos.  Customers are responsible for their own applications hosted in Microsoft Azure. |
| **Q. 109A:**  AS-1.0  AS-3.0 | *Is the code review performed by an independent party?* |  | X |  | 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. |
| **Q. 109B:**  AS-1.0 | *How often is or when code review performed?* |  |  |  | Please see responses above. |
| **Q. 110:**  AS-1.0 | *Are development and production environments separated?* | X |  |  | Development and testing responsibilities for new software builds or changes to existing software are segregated and managed through restricted access to branches within the source code library and segregated development / test environments. Features and changes are developed by the Component teams, reviewed by designated Component team members and tested by the Component team members for quality assurance and compatibility with the rest of the platform. |
| **Q. 111:**  AS-1.0 | *Do developers have access to production systems?* | X |  |  | Please see response to Question #107 above. |
| **Q. 112:**  AS-1.0 | *Is production data appropriate scrambled or encrypted used in development environments?* |  |  | X | Production / customer data is not used in development or test environments. |
| **Q. 113:**  AS-1.0 | *What private or sensitive data or content is kept?* |  |  |  | Microsoft Azure personnel may only access customer data when required to resolve a customer reported incident, security incident or a live site incident. For all such accesses, there is either a system-adjudicated scenario, based on JIT policy (handled by JIT), or the following has to be in place:   1. There is a work item describing the reason. 2. The incident has a record of approval (e.g. email attachment) for the access. The approval can be granted by one of the following:    * Customer    * Microsoft Azure Operations Management    * Designated component team approver 3. Microsoft Azure Operations Management must have evaluated the legitimacy and business justification and grant approval only if no other means exist to resolve the incident 4. The incident should have a record of what data was accessed (but not a copy and paste of the actual data) 5. The incident should have a confirmation that secondary copies of the data, if any, have been deleted before the incident is closed.   Microsoft Azure Service engineering team personnel may need to access customer secrets such as Microsoft Azure Storage Account Keys, service management certificates, certificates that are part of the hosted service, or a remote desktop password to the customer’s VM to resolve a customer reported incident. For all such access, the same requirements for accessing customer content apply, except that only the customer can grant approval. |
| **Q. 114:**  AS-1.0 | *Do you have a data retention policy?* | X |  |  | In our Online Services Terms, Microsoft contractually commits to specific processes when a customer leaves the service or the subscription expires. This includes deleting customer data from all systems under our control.   * If you, the customer, terminate your subscription or it expires (except for free trials), Microsoft will store your customer data in a limited-function account for 90 days (the retention period) to give you time to export the data or renew your subscription. During this period, Microsoft provides multiple notices, so you will be amply forewarned of the upcoming deletion of data. * After this 90-day retention period, Microsoft will disable the account and delete all customer data, including any cached or backup copies. For in-scope services and Azure services, that deletion will occur within 90 days of the end of the retention period. (In-scope services are defined in the Data Processing Terms section of our Online Services Terms.)   In the multitenant environments of Microsoft enterprise cloud services, we take careful measures to logically separate customer data to help prevent one customer’s data from leaking into the data of another customer, as well as to help block any customer from accessing another customer’s deleted data. |
| **Q. 115:**  AS-1.1 | *What platforms are tested for security?* |  |  |  | All systems, services, applications, and environments are continuously tested and monitored for compliance with SDL practices. |
| **Q. 116:**  AS-1.3 | *How do you track bugs and remediation?* | X |  |  | The Security Development Lifecycle (SDL) is a security assurance process that is focused on software development – it applies to all Microsoft software, service and device releases.   All Microsoft Azure teams that develop code must follow SDL. SDL applies to any system or code that is available to customers as part of Microsoft Azure; or, is deployed in Microsoft Azure production to support, development and release systems; and, also includes test code that can access production resources that customers cannot access.  The following pillars have been introduced to enable agility and reduce unnecessary processes in Microsoft Azure:   1. **SDL is always current** – SDL work must be completed as part of regular development and release processes on a continuous basis. This means that teams answer security questions in security reviews, run SDL tools and fix security bugs, as per the SDL Online Services security bar, on a continuous basis, ensuring all procedures are always compliant with SDL policy or have an approved exception. During release, in the Release Signoff Record, feature teams self-attest that they have completed the SDL requirements.  This approach balances frequency of evidence collection requirements and helps teams avoid requesting exceptions to complete the mandatory engineering deliverables. It also addresses the compliance and security requirement of confirming SDL processes are completed before code is released. 2. **SDL tools are optimized to deliver at a fast release cadence** - SDL build/code tools automatically run as part of the Microsoft Azure code/build validation process. In addition, Microsoft Azure Service engineering teams can triage and analyze SDL build errors. These optimizations allow teams to complete SDL at a quicker pace. 3. **SDL process decentralized to deliver at a fast release cadence** - The process removes the burden and process steps to get SDL-related approval from ‘central teams’ (outside of their own management) before shipping. Feature teams follow best security practices including conducting security reviews (Microsoft Azure teams can request and receive support from Microsoft Azure security reviewers for help on security) before release. Instead of requiring approvals from central teams in the middle of the release process, central teams help educate, and provide a level of security analysis based on risk. |
| **Q. 117:**  AS-1.4 | *Do you provide training and user guides on additions and changes to the applications?* | X |  |  | The C+E Security Education and Awareness Program is an ongoing process by which Staff and Contingent Staff must be made aware of their security roles and responsibilities and actively help Microsoft Azure deliver more secure products and services. Therefore, the organization’s Staff and Contingent Staff need knowledge and resources to help them perform their roles securely and prevent malicious behavior.   In a typical cycle, planning and content development for training occurs after the annual Risk Assessment process. The organizational risks identified via this process serve as input into content development for that particular year’s training objectives. If it is determined that changes to the existing course content are needed, a project will be initiated. The project will implement the necessary changes prior to launching the course broadly to the organization.   Once the course is ready for launch, a point-in-time snapshot will be taken of groups in scope for the year’s training cycle. The underlying list of personnel will be the basis for measuring progress against the participation target.   Prior to granting access to the production environment, personnel are required to complete a security training course. |
| **Q. 118:**  AS-2.0 | *Do you prohibit the use of duplicate user IDs?* | X |  |  | Microsoft Azure leverages both the MCIO and Microsoft Corporate Active Directory (AD) systems, managed by MCIO and Microsoft IT respectively to control access to key information systems. Microsoft Azure personnel are assigned unique corporate AD accounts by Microsoft IT as part of standard new employee on-boarding to Microsoft. All standard access requests and approvals are managed through the Identity Management Tool or Forefront Identity Manager, which are automated workflow management tools that track the process for account request, approval, creation, modification, and deletion. |
| **Q. 119:**  AS-2.0 | *Do you provide for strong passwords and lockout controls?* | X |  |  | Applies to:   * Minimum password length of 8 characters * Minimum of 3 of the following parameters: upper case, lower case, numeric, and special characters * Maximum password age of 90 days * Minimum password age of 1 day * Maximum invalid logon attempts of between 3 and 5 attempts * User accounts locked after invalid logon attempts must be manually unlocked, and should not automatically unlock after a certain amount of time has passed * Password history of ten previous passwords |
| **Q. 120:**  AS-2.5 | *Do you store passwords in a secure manner (not in plain text, but in salted hashes, etc.)?* | X |  |  | The certificates, keys and other credentials used for internal communication amongst Microsoft Azure components such as the Fabric Controller (FC), Fabric Front-end (FFE), Fabric Agent (FA), Portal, and orchestration services are stored in the Microsoft Azure secret store for use in deployment. The Secret Store Service stores and manages credentials used by Microsoft Azure platform components. The secrets are typically stored in various component certificate stores during run-time.   The following are some capabilities of Secret Store that are relevant to cryptographic key management:   Security:   * Access to Secret Store is over an encrypted channel * Cryptographic key information is stored in an encrypted form * Tamper resistant auditing of all accesses to the secret store   Automated Key Management:   * Automatic generation of key pairs and certificates * Automatic and secure storage of the key pair information in a database * Automatic on-demand, minimal downtime key rollovers   Alerting and Reporting:   * Alerting on certificates that will expire in next N days. |
| **Q. 121:**  AS-2.5 | *Are passwords transmitted in a secure manner (e.g. over TLS or other encrypted protocols)?* | X |  |  | See answer to question #120 above.  Password policies for corporate and MCIO domain accounts are governed through the respective Microsoft corporate and MCIO AD policies that specify minimum requirements for password length, complexity and expiry. |
| **Q. 122:**  AS-2.0 | *Do you provide for directory services to perform authentication?* | X |  |  | Microsoft Azure leverages both the MCIO and Microsoft Corporate Active Directory (AD) systems, managed by MCIO and Microsoft IT respectively to control access to key information systems. Microsoft Azure personnel are assigned unique corporate AD accounts by Microsoft IT as part of standard new employee on-boarding to Microsoft. All standard access requests and approvals are managed through the Identity Management Tool or Forefront Identity Manager, which are automated workflow management tools that track the process for account request, approval, creation, modification, and deletion. |
| **Q. 123:**  AS-2.0 | *Do you provide for multi-factor authentication?* | X |  |  | Azure Multi-Factor Authentication (MFA) implements least-privilege giving users and systems the minimum level of access necessary to perform their defined functions. All users must be explicitly authorized prior to being granted access, and have the most restrictive level of access that still permits accomplishment of their job responsibilities. This is accomplished within MFA by the utilization of security group membership and local accounts where the membership is reviewed and audited to ensure that only persons requiring that level of access are included in the security group membership. For the tools having local accounts, the access to the local accounts is granted to only those personnel who have valid business justification for the services accessed. |
| **Q. 124:**  AS-2.0 | *Do you use an Identity and Access Management (IAM) system to initiate, capture, record, and manage users and their access permissions?* | X |  |  | Azure AD / AD Federation Services, Microsoft corporate AD, Forefront Identity Manager for Microsoft employee and contractor access control.  Azure also provides detailed audit reporting of AD usage, and all management-level access is continuously monitored and audited. |
| **Q. 125:**  AS-2.1 | *Do you provide for the registration of devices by application users and the checking of devices used against a list of known registered devices?* | X |  |  | Service accounts are configured by the GNS team to enable a Microsoft Azure client to authenticate to network devices – specifically, the routers, TOR switches, and load balancers. Accounts are created on a per-process/application basis and are configured by GNS. The accounts are configured with the required access for their purpose by GNS and, if required, authentication spans datacenters.   Microsoft Azure Managed Devices (Digis and PDUs): Digi CMs and PDUs accounts are managed through automation and are maintained within the Secret Store repository. Managed devices can be accessed through a defined subset of systems. |
| **Q. 125A:**  AS-2.1 | *What do you register devices by?* |  |  |  | Applies to: device or hardware ID, IMEI or MEID, MAC address, IP address, other:  Devices on the Microsoft Azure network authenticate with unique identifiers in the form of static MAC addresses and certificates. A physical node or VM obtains an IP address over the network when it initially boots-up. The Fabric DHCP Server is responsible for assigning IP addresses to Physical Nodes and VMs as determined by the Fabric Controller. This allows the Fabric Controller to take control of managing the IP address pools for the set of Physical Nodes. IP filters on the host operating system are programmed via the Fabric to only allow traffic from specific MAC addresses and specific DIPs, to counter ARP spoofing. |
| **Q. 125B:**  AS-2.1 | *Do you limit the number of devices per user?* |  |  | X | There are no user devices on the Azure production network, as there are no direct-connect wireless networks in Azure datacenters. Approved access is allowed from user devices from the Microsoft corporate network only, and any such devices have encryption and access policies enforced. |
| **Q. 125C:**  AS-2.1 | *Do you restrict multiple simultaneous sessions?* |  |  | X | Azure's DDoS defense system employs multiple mechanisms to monitor and detect anomalous session and network activity. Continuous monitoring systems analyze traffic and perform event correlation along with integrated IDS. |
| **Q. 126:**  AS-2.2 | *Describe your password recovery procedures. (Please specify in the comments box to the right)* |  |  |  | Password policies for corporate domain accounts are managed through the Microsoft corporate AD policy that specifies minimum requirements for password length, complexity and expiry. Temporary passwords are communicated to users using Microsoft IT established processes. Guidelines for password selection and use has been defined and published in Online Services Security Standards.  Corporate password policies are of particular note in authentication management:   * Change or refresh of authenticators by MSIT every 70 days * Enforce passwords with a minimum of eight characters   Per Microsoft’s Access Control Policy, passwords are not recovered, they are only reset via established verification mechanisms. |
| **Q. 127:**  AS-2.3 | *Do your application(s) run under least privilege? (Not under administrator, system, or root)* | X |  |  | All account access (including user, application, and system) is Security-group driven and follows a least-privilege model. Access must be requested and received for appropriate purposes using just-in-time and least-access policies. |
| **Q. 128:**  AS-2.5 | *Do you have a key management lifecycle?* | X |  |  | Key Management encompasses the entire lifecycle of cryptographic keys. A key has three phases during its life, namely Pre-Operational, Operational and Post-Operational.  Pre-Operational Phase:   * **Key Generation**—When a component team needs a new self-signed certificate, they are able to generate it using Secret Store. Secret Store generates the certificate, stores it and makes the metadata available to the requestor. * **Key Installation**—Component teams use the metadata of the certificate and invoke Secret Store to install the certificate on Fabric Nodes, MDS Runners, or Tenants. Typically, this is performed as part of the deployment process. * **Key Storage**—Keys are stored in the Secret Store database in an encrypted format. Secret Store automatically (and securely) populates the Secret Store Service database with the new public and private key info, including setting the initial access control policy for this data. * **Master Encryption Certificate**—The master encryption certificate is in non-exportable form on the administrators’ account of the secret store machine. The Administrator access to secret store machine is restricted to administrators from WAPS FTE staff.   Operational Phase:   * **Key Expiry/Rotation/Change**—Certificate expiration monitoring engines have been deployed within Microsoft Azure Services. As a monitoring engine detects an expiring certificate, a new Secret Expiration entry will be created in the tracking system. Component teams manage the Rotation Periodicity along with self-reporting to ensure compliance. * **Key Compromise**—In case of a key compromise, an incident ticket is created, and the issue is escalated to operations managers. Based on the extent of compromise and the impact, the existing certificate and the service may be brought down temporarily. A new certificate is created and the deployment is carried out in accordance with the release/change management process. Microsoft Azure Live Support (ALS) notifies the Certificate Authority of the certificate that’s revoked, then the component team updates the component’s configuration as necessary such that it refers to the new, rather than the old, certificate.   Post-Operation Phase:   * **Key Revocation**—In case a key needs to be revoked due to a key compromise, Key Compromise procedure should be followed. * **Key Archival and Recovery**—All keys are stored for two years after they are marked deleted in the Secret Store and are recoverable if needed. In case the key needs to be recovered, a ticket is raised and the Secret Store administrator recovers the key. * **Key Destruction**—In the case of key destruction for the master encryption certificate, the keys stored in physical locations are wiped securely in such a way that they can’t be recovered. * **Logging & Auditing**—The Secret Store uses an audit agent to detect actions taken on the Secret Store machine. This includes process execution, terminal service sessions, login session, network connections etc. The audit agent also sends these events to the monitoring agent stream. The Secret Store also logs all actions invoked using its frontend to the local database and an event stream.   The Secret Store uses MDS. The monitoring agent runs on the Secret Store machine, and uploads the QoS alarm and audit events to Azure Storage. These events are available to MDS to carry out monitoring of the Secret Store system. |
| **Q. 129:**  AS-2.5 | *Do you protect keys in a vault?* | X |  |  | Keys are stored in the Secret Store database in an encrypted format. The Secret Store automatically (and securely) populates the Secret Store Service database with the new public and private key information, including setting the initial access control policy for this data. |
| **Q. 130:**  AS-2.5 | *Do you store key away from the data they are used to encrypt?* | X |  |  | Key Vault is physically separated (for Secret Store) from applications hosting platform and customer data. |
| **Q. 131:**  AS-2.5 | *Do you distribute keys separately (out-of-band) from the data?* | X |  |  | Security:   * Access to Secret Store is over an encrypted channel * Cryptographic key information is stored in an encrypted form * Tamper-resistant auditing of all accesses to Secret Store   Automated Key Management:   * Automatic generation of key pairs and certificates * Automatic and secure storage of the key pair information in a database * Automatic on-demand, minimal downtime key rollovers   Alerting and Reporting:   * Alerting on certificates that will expire in next N days. |
| **Q. 132:**  AS-2.5 | *Do you create unique encryption keys per tenant?* | X |  |  | This is a user control, as customers can bring their own keys or use Key Vault (or other mechanism) to implement unique keys as needed. |
| **Q. 132A:**  AS-2.5 | *Do you create unique encryption keys per project?* |  |  | X | This is a user control, as customers can bring their own keys or use Key Vault (or other mechanism) to implement unique keys as needed. |
| **Q. 133:**  AS-2.5 | *Do you revoke keys or rekey data every one to three years?* | X |  |  | Secrets rotation (certificates, storage account keys, passwords, tokens, database connection strings, etc.) is followed per the documented Azure Encryption standard operating procedure (SOP) and is dependent on the individual service or encryption mechanism. |
| **Q. 134:**  AS-2.5 | *Do you segregate duties for creating, managing, and using keys?* | X |  |  | Azure security groups (role-based access control) are used for PKI management, and only approved entities may make changes based on JIT access. |
| **Q. 135:**  AS-2.5 | *Is key creation logged and reviewed?* | X |  |  | The Secret Store uses an audit agent to detect actions taken on the Secret Store machine. This includes process execution, terminal service sessions, login session, network connections etc. The audit agent also sends these events to the monitoring agent stream. The Secret Store also logs all actions invoked using its frontend to the local database and an event stream.   The Secret Store uses MDS. The monitoring agent runs on the Secret Store machine, and uploads the QoS alarm and audit events to Azure Storage. These events are available to MDS to carry out monitoring of the Secret Store system. |
| **Q. 136:**  AS-2.6 | *Do you implement auto-expiration for external links to content?* |  |  | X | This is a user control. Azure does not publish customer data automatically, and secure access must be configured by the customer. The Azure production network does not link to external networks except as defined and managed by the subscriber. Azure Portal links to external information, such as partner website URLs in the Azure Marketplace, are maintained by their respective owners. |
| **Q. 137:**  AS-2.7 | *Do you utilize CAPTCHA or reCAPTCHA to protect against bots* |  |  | X | Azure MFA is available to customers for implementing tamper-resistant authentication. |
| **Q. 138:**  AS-2.9 | *Do you send e-mail immediate to content owners, project owners, or mangers whenever content is uploaded, downloaded, or viewed?* |  |  | X | This is a customer control, but detailed monitoring and auditing is available through Azure AD for access management, Azure Storage, and other services through Azure's diagnostic services and Security Center. |
| **Q. 139:**  AS-2.9 | *Do you record the following details for upload or download of content?* |  |  | X | This is a customer control, but detailed monitoring and auditing is available through Azure AD for access management, Azure Storage, and other services through Azure's diagnostic services and Security Center. |
| **Q. 140:**  AS-2.10 | *Do you have a mobile device management system?* |  |  | X | For corporate-connected approved devices, AD group policies mandate device health and screening. Mobile devices cannot connect directly to the Azure production environment. |
| **Q. 141:**  AS-3.0  AS-3.1 | *Do you have a vulnerability management process to cyclically identify, classify, remediate, and mitigate security vulnerabilities on networking and computing devices, and applications?  If yes, how often are vulnerabilities tested for? What is the interval between tests or vulnerability management cycles? (Please specifiy in the comments box)* | X |  |  | Procedures have been established and implemented to regularly scan for vulnerabilities on hypervisor hosts. Vulnerability scanning is performed on server operating systems, databases, and network devices with the appropriate vulnerability scanning tools. The vulnerability scans are performed on a quarterly basis at a minimum. Azure contracts with independent assessors to perform penetration testing of the Azure boundary. Red Team / Blue Team exercises are also routinely performed and results used to make security improvements. |
| **Q. 141A:**  AS-3.0  AS-3.1 | *How often are tests performed by independent third parties?* |  |  |  | Quarterly. |
| **Q. 142B:**  AS-3.0, AS-3.1 | *How do you prioritize remediation of vulnerabilities?* |  |  |  | The Microsoft Security Response Center (MSRC) publishes security bulletins and associated patches and security advisories. Third party vulnerabilities are addressed as they are discovered via scanning in the environment.   Azure Security Engineering assesses impact and determines the required patching schedule in consultation with key security teams across Microsoft. The triage process includes an initial vulnerability risk assessment tool that helps prioritize resourcing and responding to identified risks. This risk management technique is designed to help:   1. Manage threats and vulnerabilities in a structured, repeatable format 2. Produce an early view into both business impact and threat likelihood to determine overall risk 3. Identify and prioritize remediation and mitigation actions for implementation 4. Focus information security resources to best effect.   Triage is conducted monthly and ad-hoc as needed when new vulnerabilities are discovered. Because analysis results are used to determine mitigation and remediation activities, analysis is conducted as soon as possible to allow the business to respond effectively. The volume of newly discovered vulnerabilities can vary widely, resulting in an unpredictable drain on resources. The triage process reduces this unpredictability by allowing the analyst to prioritize detailed analysis work for those vulnerabilities that are most likely to require either detailed planning or an immediate response.  As new vulnerabilities are identified though scanning and other means, Azure Security Engineering measures exploitability (ability for a malicious actor to easily and reliably take advantage of the vulnerability) and remediation capability (the ability for an Asset Owner to easily address the vulnerability). These factors combine to create a triage score, indicating which vulnerabilities require additional detailed analysis. |
| **Q. 143:**  AS-3.3 | *Do you validate and/or sanitize input and implement secure error handling (respond to incorrect user input with safe error messages, i.e. messages that not give away information that a malicious user might find helpful in attacking the system)?* | X |  |  | 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 are 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. |
| **Q. 144:**  AS-3.4 | *Do you implement logging procedures?  If yes, what events do you log? What attributes are contained in the logs?* | X |  |  | Logging, real-time monitoring and alerting is enabled for service health diagnostics and for security.   * Service teams define the requirements for logging of diagnostics events to support service health to ensure information system problems are identified * The C+E Security team defined the requirements for security logging and monitoring for security events of interest to aid in security incident investigations   To support this, logging and monitoring is enabled at each layer of the service:   * Service Application   + Audit logs   + Diagnostics Logs   + Service application monitors and alerts * Infrastructure   + IIS logs   + OS Security events   + Audit logs for management tools   + Infrastructure monitors and alerts * Network/Firewall   + ACLs and firewall settings   + Syslogs for devices   + Network monitors and alerts |
| **Q. 145:**  AS-3.5 | *Do you have an SIEM (Security Information Event Management System) to aggregate and analyze the disparate logs?*  *What functions are provided by the SIEM?* | X |  |  | Applies to:   * Centralized event log repository for data/event log aggregation from servers, systems, applications and infrastructure devices * Automated correlation of multiple isolated security events to a one single, relevant security incident * Alerting to notify the security team of immediate issues * File-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts * Alerting to indicate concurrent logons * Other:   Security logging in Azure is both robust and varied, and operates continuously. |
| **Q. 146:**  AS-3.6 | *Do you encrypt content and client data at rest?* | X |  |  | Azure provides comprehensive isolation, RBAC and at-rest encryption options for customer data. However, customers must configure encryption or other data protection mechanisms for their subscription environments. For more information, see <http://download.microsoft.com/download/0/D/D/0DD8FB12-6343-4A50-80B2-545F2951D7AE/MicrosoftAzureDataProtection_Aug2014.pdf> |
| **Q. 147:**  AS-3.7 | *Do you implement the following controls for session management (connection)?* | X |  |  | Applies to:   * TLS 1.0 or better * Appropriate certificate authority * No wildcard certifications * Full qualified names in certificates * Other:   Perfect Forward Secrecy |
| **Q. 148:**  AS-3.8 | *Do you implement the following controls for session management (session ID)?* | X |  |  | Applies to:   * Use a secure session name that does not reveal unnecessary details such as user name/ID, token, the platforms used * Use a long enough session ID to prevent brute force attacks * Use unpredictable random session IDs * Use strict session management whenever possible * Validate and filter out any invalid session ID’s before processing them * Renew the session ID after any privilege level change * Limit session ID exchange mechanisms (e.g., cookies or URL parameter) * Implement an idle timeout for every session * Set mandatory expiration timeouts for every session * Include manual session expiration (e.g., logout button). Force session logout on web browser window close.   Note that Azure follows SDL for all application development, and implements best-practices according to the OWASP Top-10 and other accepted industry best practices. |
| **Q. 149:**  AS-3.9 | *Do you implement the following controls to prevent SQL injection?* | X |  |  | Applies to:   * Use prepared statements * Use stored procedures * Escape all user-supplied input * Minimize the privileges assigned to database accounts * Validate input using whitelisting * Other:   See above answer for AS-3.8. |
| **Q. 150:**  AS-3.10 | *Do you implement the following controls to prevent invalid URL redirects and forwards* | X |  |  | This is a customer control, to be implemented in the customer's web application.  The Azure Portal is designed according to SDL best-practices. |
| **Q. 151:**  AS-3.11 | *Do you implement controls to prevent connections from anonymity networks (e.g., Tor, Freenet, Netshade)?* |  | X |  | Microsoft does not regulate customer connections to their environments. Customers must implement appropriate security mechanisms and controls to block unwanted network traffic. Azure does provide tools and mechanisms by default, such as firewalls and packet filters, but the customer should configure their access rules to only allow desired traffic. We also recommend the use of third-party access gateways, IDS, application firewalls, etc. |
| **Q. 152:**  AS-3.12 | *Do implement controls to prevent IP address leakage?* | X |  |  | Azure infrastructure self-manages host IPs and network configurations. Customers must implement suitable controls within their Virtual Networks to prevent network-based attacks, as indicated in AS-3.11 above. |
| **Q. 153:**  AS-3.13 | *Do you implement the following controls to prevent XSS?* | X |  |  | Applies to:   * Disallow insert untrusted data, except in allowed locations * HTML Escape before inserting untrusted data into HTML element content * Attribute Escape before inserting untrusted data into HTML common attributes * JavaScript Escape before inserting untrusted data into JavaScript data values * CSS Escape and strictly validate before inserting untrusted data into HTML style property values * URL Escape before inserting untrusted data into HTML URL parameter values * Sanitize HTML markup with a library * Prevent DOM-based XSS * Use the HTTPOnly cookie flag, when possible (e.g., JavaScript is not in use) * Other:   Note that Azure follows SDL for all application development, and implements best-practices according to the OWASP Top-10 and other accepted industry best practices. |
| **Q. 154:**  CS-1.3 | *Do you have documented security baselines for components of the infrastructure (hypervisors, operating systems, routers, etc.)?* | X |  |  | The baseline configuration lifecycle defines a repeatable process by which baselines are established, evolved and monitored. Five distinct stages create a framework for managing the lifecycle of a baseline: (Establish) Update Baseline, Adoption / Deployment, Scan, Report, Review / Analysis (Remediate).  Upon the creation of a new baseline, an initial starting point has to be established. Public consensus-based industry best practices are utilized to define an initial baseline.   The Microsoft Azure Team leverages security benchmarks from the Center for Internet Security, Inc. (CIS) to assist in the establishment of initial baselines [CIS website: <http://benchmarks.cisecurity.org>].  Microsoft Azure product and technical subject matter experts review the CIS benchmarks and where appropriate customize the base settings for the Microsoft Azure environment. This customization may include the addition or removal of rules or rule update from the CIS benchmark. Upon completion of this review and customization, the initial baseline is presented for approval. Once approved, the initial baseline is established.   Throughout the lifecycle process, needs to update the baseline are identified, reviewed and approved. These needs may be identified from (i) outputs from the “review / analysis” stage and (ii) updates from CIS. |
| **Q. 155:**  AS-3.14 | *Do you allow senders the option to include session-based forensic (invisible) watermarking for content?* | X |  |  | Customers may encode digital assets as dictated by their business needs. Azure does not pre-process or restrict content that customers upload or stream. |
| **Q. 156:**  AS-3.14 | *Do you verify and test the strength of the forensic watermark on a regular basis?* |  | X |  | This is a customer responsibility, as Azure does not control watermarking of stored content. |
| **Q. 157:**  AS-3.15 | *Do you have a formal documented content lifecycle policy?* |  |  | X | This is a customer responsibility for data uploaded to Azure services, but Azure infrastructure has a comprehensive ISMS / ISMP which dictates storage and destruction policies. |

# Cloud Security

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Control IDs** | **MPAA Guidelines** | **Microsoft Azure Response** | | | |
| **Yes** | **No** | **N/A** | **Notes** |
| **Q. 200:**  CS-1.2 | *Do you have documented security and privacy policies?* | X |  |  | 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. |
| **Q. 201:**  CS-1.4 | *Do you have documented personnel security procedures?* | X |  |  | 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. |
| **Q. 202:**  CS-1.5 | *Do you require all employees, contractors, and third parties to sign confidentiality / non-disclosure agreements when going through the on-boarding process?* | X |  |  | Microsoft staff take part in a Microsoft Azure and/or MCIO-sponsored security training program, and are recipients of periodic security awareness updates when applicable. Security education is an on-going process and is conducted regularly in order to minimize risks. An example of an internal training is Microsoft Security 101. Microsoft also has non-disclosure provisions in our employee contracts.  Microsoft Azure and/or MCIO staff are required to take training determined to be appropriate to the services being provided and the role they perform. |
| **Q. 203:**  CS-1.14 | *Do you train all personnel, contractors, and third-parties regarding all policies and procedures, including their legal responsibility for security and data integrity?* | X |  |  | Microsoft Azure contractor staff and FTE staff are required to take any training determined to be appropriate to the services being provided and the role they perform.  Microsoft staff take part in a Microsoft Azure and/or MCIO-sponsored security training program, and are recipients of periodic security awareness updates when applicable. Security education is an ongoing process and is conducted regularly in order to minimize risks. An example of an internal training is Microsoft Security 101. Microsoft also has non-disclosure provisions in employee contracts. |
| **Q. 204:**  CS-1.15 | *Do you have a process to notify clients when material changes are made to security / privacy policies?* | X |  |  | Microsoft will update privacy statements when necessary to reflect customer feedback and changes in our services. When we post changes to a statement, we will revise the "last updated" date at the top of the statement. If there are material changes to the statement or in how Microsoft will use your personal data, we will notify either by prominently posting a notice of such changes before they take effect or by directly sending a notification. We encourage periodic review of privacy statements to learn how Microsoft is protecting your information. |
| **Q. 205:**  CS-1.6 | *Do you have procedures for conducting security due diligence when off-boarding functionality or services to third parties?*  *What due diligence and monitoring is being performed?* | X |  |  | Applies to:   * Documentation reviews (e.g., independent audits, logs, compliance, penetration test results, and remediation plans) * Verification of adherence to industry standards for SDLC security * Other:   Microsoft Azure business partners and third-party contractors are required to follow the same established software development and release management processes, including SDL and OSA guidelines, to control implementation of major changes as Microsoft Azure software developers. |
| **Q. 206:**  CS-1.7 | *Do you document and implement segregation of duties for business critical tasks?* | X |  |  | Segregation of duties is established on critical functions within the Microsoft Azure environment to minimize the risk of unintentional or unauthorized access or change to production systems. Duties and responsibilities are segregated and defined between Microsoft Azure operation teams. Asset owners / custodians approve different accesses and privileges in the production environment. Segregation of duties is implemented in Microsoft Azures’ environments in order to minimize the potential of fraud, misuse, or error. |
| **Q. 207:**  CS-1.7 | *Do you document compensating controls where segregation of duties is not feasible?* |  |  | X | 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. |
| **Q. 208:**  CS-1.8 | *Do you provide the client with information regarding locations for their content and data including the how data is transported and information on the content, data location, and legal jurisdictions?* | X |  |  | In regulated industries or in countries with data protection laws, customers must maintain their data in a specific geographic location, such as within the European Union or within countries that are members of the Asia-Pacific Economic Cooperation (APEC) forum.  Microsoft maintains an ever-expanding network of datacenters in locations around the globe, and verifies that each meets strict security requirements. As a Microsoft Cloud customer, you will know the location where your data is stored and control the region in which it stays: <https://www.microsoft.com/en-us/TrustCenter/Privacy/You-are-in-control-of-your-data/Azure-location> |
| **Q. 209:**  CS-1.9 | *Do you have a documented procedure for responding to requests for client data from governments or third parties?* | X |  |  | Microsoft’s Corporate, External, and Legal Affairs (CELA) Group monitors changes to regulatory requirements across all jurisdictions in which Microsoft Azure conducts business. Microsoft Azure is part of a comprehensive compliance effort at Microsoft that is expanding encryption, reinforcing legal protections, and increasing transparency.  Microsoft follows clear principles in responding to government legal demands for customer data:   * We require a valid subpoena or legal equivalent before we consider releasing a customer’s non-content data to law enforcement * We require a court order or warrant before we consider releasing a customer’s content data * In each instance, we carefully examine the requests we receive for a customer’s information to make sure they are in accord with the laws, rules and procedures that apply. |
| **Q. 210:**  CS-1.10 | *Do you have policies and procedures for labeling, handling, and securing containers that contain data and other containers?* | X |  |  | 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. |
| **Q. 211:**  CS-1.10 | *Do you follow a structured labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?* |  |  | X | Microsoft does not classify data uploaded and stored by customers. |
| **Q. 212:**  CS-1.11 | *Do you have a procedure for the secure deletion of content/data, including archived and backed-up content/data?* | X |  |  | 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. |
| **Q. 213:**  CS-1.11 | *Do data disposal procedures comply with all legal and regulatory requirements for scrubbing of sensitive content/data?* | X |  |  | 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. |
| **Q. 214:**  CS-1.12 | *Do you have documented processes for clients, in which client content/data may be moved from one physical location to another (e.g., offsite backups, business continuity failovers, and replication)?* | X |  |  | 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. |
| **Q. 215:**  CS-1.12 | *Do you disclose all movements in writing prior to the implementation?* |  | X |  | Customers are responsible for managing data location and transmission within their cloud environment. Azure provides mechanisms for constraining data location to specific geographic regions and contractually commits to keeping customer data in specified locations.  Customer data may be moved within a datacenter or region as needed by the infrastructure to maintain availability, recover from outage, or respond to a service incident. Data moved by Azure is always done so over an encrypted channel, but the customer may not be notified of such moves managed by automatic processes. |
| **Q. 216:**  CS-1.13 | *Do you have the following key management policies and procedures?* | X |  |  | Applies to:   * Use of strong encryption for moving client content * Segregation duties for creating, managing and using keys * Not storing keys in the cloud * Other:   Microsoft has policies, procedures, and mechanisms established for effective key management to support encryption of data in storage and in transmission for the key components of the Microsoft Azure service.  Microsoft provides customers the option of encrypting customer data transmitted to and from Microsoft data centers over public networks. Microsoft uses private networks with encryption for replication of non-public customer data between Microsoft data centers.  Microsoft Azure implements the transmission integrity and confidentiality control by ensuring that the cryptography is implemented through a hybrid model using both symmetric and asymmetric keys for encrypting and protecting confidentiality of data, which at a high-level are:   * Use AES for symmetric encryption/decryption * Use 128-bit or better symmetric keys * Use RSA for asymmetric encryption/decryption and signatures * Use 2048-bit or better RSA keys * Use SHA-256 or better (SHA-384, SHA-512) for hashing and message-authentication codes |
| **Q. 217:**  CS-1.16 | *Do you plan, prepare, and measure the following system performance to ensure acceptable service levels?* | X |  |  | Applies to:   * Availability of service * quality of service * capacity planning * continuous performance monitoring * Other:   The Microsoft Azure Capacity Management team projects future usage capacity requirements and provisioning for disaster recovery using the following:   * Demand model based on revenue forecasts * Weekly or monthly cadence reports which is a scorecard of technical subscription information * Internal use reports e.g. top 10 customer reports, daily ad-hoc checks, daily surge reports which are shared and discussed with the Capacity Planning team * Inputs from component teams on capacity requirements   Thresholds for safe limit usage are defined with inputs from the component teams, with real-time monitoring of the cluster against those thresholds. |
| **Q. 218:**  CS-1.17 | *Do you have incident response policies and procedures for immediate notification to the client in the event of any unauthorized access to systems and content?* | X |  |  | Microsoft Azure provides security incident response training to personnel identified in the incident response plan on an annual basis. Microsoft Azure has established and published an incident response plan with defined procedures, roles and responsibilities for monitoring, detection, response and post-mortem of incidents. The incident response plan is reviewed on an annual basis for continued accuracy and completeness. Microsoft's Developer Network and Azure Security provide support and guidance to customers on information security incidents related to their cloud environment. |
| **Q. 219:**  CS-2.0 | *Do you properly secure datacenter services and environmental conditions by performing the following activities:* | X |  |  | Applies to:   * Monitoring * Maintenance * Testing of security controls at least annually * Other:   Azure datacenters have dedicated 24x7 uninterruptible power supply (UPS) and emergency power support, which may include generators. Regular maintenance and testing is conducted for both the UPS and generators. Datacenters have made arrangements for emergency fuel delivery.  The datacenter has 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. * The Heating, Ventilation and Air Conditioning (HVAC) system, which controls and monitors space temperature and humidity within the data centers, space pressurization and outside air intake.   Fire Detection and Suppression systems exist at all datacenters. Additionally, portable fire extinguishers are available at various locations in the datacenter. Routine maintenance is performed on facility and environmental protection equipment. |
| **Q. 220:**  CS-2.1 | *Do you ensure the datacenter has appropriate perimeter and physical security controls?* | X |  |  | 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 Datacenters. Front desk personnel are required to positively identify Full-Time Employees (FTEs) or authorized Contractors without ID cards. Staff must wear identity badges at all times, and are required to challenge or report individuals without badges. All guests are required to wear guest badges and be escorted by authorized Microsoft personnel.  In addition to the physical entry controls that are installed on various doors within the datacenter, the Microsoft Datacenter Management organization has implemented operational procedures to restrict physical access to authorized employees, contractors and visitors.  Datacenter buildings are nondescript and do not advertise that Microsoft Datacenter hosting services are provided at the location. Access to the datacenter facilities is restricted. The main interior or reception areas have electronic card access control devices on the perimeter door(s), which restrict access to the interior facilities. Rooms within the Microsoft Datacenter that contain critical systems (servers, generators, electrical panels, network equipment, etc.) are restricted through various security mechanisms such as electronic card access control, keyed lock, anti-tailgating and/or biometric devices. |
| **Q. 221:**  CS-2.2 | *Do you have a business continuity plan, process, and procedures?* | X |  |  | Continuity risks are identified, documented and communicated within the Microsoft Azure teams. Microsoft Azure has conducted a risk assessment and loss scenarios (e.g., servers, facilities, building, campus, etc.) analysis to identify continuity risks related to Microsoft Azure services.  The Business Impact Analysis is carried out based on the approved framework. Impacts are assessed on revenue (existing customer turnover and future customers) and operations (customer / partner experience, brand / shareholder value, 3rd party agreements, legal & regulatory requirements, employee and workforce) for critical services. Critical services are identified through discussions with Microsoft Azure management and subject matter experts. The initial critical services identified include:   1. Storage data 2. Compute service 3. Service management 4. Storage service 5. Edge compute   Microsoft Azure has also conducted a technical (e.g. servers, network, storage) and non-technical (e.g. processes, suppliers) dependencies analysis to identify critical dependencies on systems, processes and supporting functions. As part of the technical dependency analysis, assets supporting critical services have been identified and documented.  The customer is also responsible for performing these duties. |
| **Q. 221A:**  CS-2.2 | *Do you test backup, recovery, and redundancy processes tested at least quarterly?* | X |  |  | Business Continuity Plans (BCPs) have been documented and published for critical Azure services, which provide roles and responsibilities and detailed procedures for recovery and reconstitution of systems to a known state per defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Plans are reviewed on an annual basis, at a minimum.  The BCP team conducts testing of the business continuity and disaster recovery plans for critical services, per the defined testing schedule for different loss scenarios. Each loss scenario is tested at least annually. Issues identified during testing are resolved during the exercises and plans are updated accordingly. |
| **Q. 222:**  CS-2.3 | *Do you perform change control when making software or hardware changes to applications and systems?* | X |  |  | 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.   Azure teams review and update configuration settings and baseline configurations of hardware, software and network devices at least annually. Changes are developed, tested and approved prior to entering the production environment in a development and/or test environment.   The customer is also responsible for performing these duties. |
| **Q. 223:**  CS-2.4 | *Do you maintain an inventory of all critical assets, including ownership of the asset?* | X |  |  | Major assets used to support the delivery of Azure's services must be accounted for and have an identified owner. The Asset Owner is accountable for maintaining a complete inventory of their major assets, and providing the appropriate level of protection for each asset throughout its existence. The inventory must clearly identify, at a minimum, each asset's owner, current location, and security classification.   Microsoft Azure maintains a detailed inventory of assets within its authorization boundary which is documented and audit-ready. Microsoft Azure employs automated mechanisms to detect and troubleshoot exceptions or deviations from the baseline configuration in the production environment. In addition, Microsoft Azure Fabric Controllers are programmed to only allow authorized components to operate and transmit within its environment.  The customer is also responsible for performing these duties. |
| **Q. 224:**  CS-2.5 | *Do you maintain an inventory of all critical supplier relationships?* | X |  |  | All supplier relationships with Azure are tracked and all suppliers audited on an annual basis.   The customer is also responsible for performing these duties. |
| **Q. 225:**  CS-2.6 | *Do you maintain service level agreements (SLA's) with clients, partners, and service providers?* | X |  |  | Any third party outsourcing must follow Microsoft’s corporate procurement process. Additional risks applicable with third party vendors having access to customer information or production access must be documented.   The managers of Microsoft Azure teams, who engage or oversee third party service providers, are responsible for the following:   1. Adhering to Microsoft Global Procurement processes and working with the Server and Tools Business (STB) Procurement contacts, for selecting and engaging third parties; 2. Engaging Legal and Corporate Affairs (LCA) to ensure appropriate contractual agreements are in place prior to entering into discussions with third parties and granting them access to information systems; 3. Ensuring the resources of the Microsoft Azure third party service providers, and other third parties are in compliance with the Microsoft Azure Information Security Policy; 4. Providing third party personnel with appropriate information and training on Microsoft and Microsoft Azure security requirements, including guidelines and procedures relevant to their job responsibilities; 5. Restricting and removing access of third party personnel to Microsoft Azure information systems and assets commensurate with the job responsibilities and duration of the services provided. 6. Monitoring and reviewing third party service providers’ performance and compliance with security requirements regularly.   Microsoft Azure has established procedures and designated responsibilities for managing changes to third-party services. Microsoft Azure's designated teams manage third-party relationships including contract management, monitoring metrics such as service-level agreements, and third party access to systems, in accordance with these procedures as well as corporate-wide third-party management processes.  Prior to engaging in Microsoft 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.  The customer is also responsible for performing these duties. |
| **Q. 226:**  CS-3.0 | *Do you have a process for providing all relevant logs to the client, in the event of a security incident, if requested by the client?* | X |  |  | Microsoft Azure Diagnostics enables the collection of diagnostic data from an application running in Microsoft Azure. Diagnostic data may be used for debugging and troubleshooting, measuring performance, monitoring resource usage, traffic analysis and capacity planning, and auditing. After the diagnostic data is collected it can be transferred to a Microsoft Azure Storage account for persistence. Transfers can either be scheduled or on-demand. Azure Diagnostics is configured using an XML configuration file.   The Azure Threat Management Team utilizes a variety of tools to monitor system events. ACS is used to retrieve Windows security event logs from:   * IaaS servers * Domain controllers in the MCIO-Managed domains supporting the IaaS Security Authorization boundary.   Microsoft Azure platform components (including OS, Fabric, etc.) are configured to log and collect security events. Administrator activity in the Microsoft Azure platform is logged.  The customer is responsible for establishing proper log settings and for ensuring secure log transport. |
| **Q. 227:**  CS-3.1 | *Do you have the capability to provide system geographic location as an additional authentication factor?* |  | X |  | This feature is not yet implemented. |
| **Q. 228:**  CS-3.2 | *Do you have the capability to control the physical location/geography of storage of client's content/data, if requested?* | X |  |  | 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.  The customer is also responsible for performing these duties. |
| **Q. 229:**  CS-3.3 | *Do you have a process and procedure to ensure that non-production data is not replicated to production environment (i.e., the segregation of non-production data from production data) and vice versa?* | X |  |  | 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 duty 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. |
| **Q. 230:**  CS-3.4 | *Do you have a process for exiting the service arrangement with a client, which includes the assurance to sanitize all computing systems of the client content/data once the client contract is terminated?* | X |  |  | 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.  The customer is also responsible for performing these duties. |
| **Q. 231:**  CS-3.5 | *Do you have policies and procedures for the secure disposal of equipment, categorized by asset type, used outside the organization's premises?* | X |  |  | 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 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.  The customer is also responsible for performing these duties. |
| **Q. 232:**  CS-3.6 | *Have you implemented a synchronized time service protocol (e.g., NTP) to ensure all systems have a common time reference?* | X |  |  | Azure 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. |
| **Q. 233:**  CS-3.7 | *Do you monitor and restrict traffic between trusted and untrusted connections, including network domains and zones within network and virtual environments?* | X |  |  | Azure provides network isolation for each deployment. Using input endpoints, customers decide which ports can be accessed from the Internet. · Traffic between VMs always traverses through trusted packet filters.   1. Protocols such as Address Resolution Protocol (ARP), Dynamic Host Configuration Protocol (DHCP), and other OSI Layer-2 traffic from a VM are controlled using rate-limiting and anti-spoofing protection. 2. VMs cannot capture any traffic on the network that is not destined to it.    * Customer VMs cannot send traffic to Azure’s private interfaces or other customers’ VMs, or Azure infrastructure services themselves.    * Customer VMs can only communicate with other VMs owned or controlled by the same customer and with Azure infrastructure service endpoints meant for public communications.    * When customers put VMs on a virtual private network, those VMs get their own address spaces that are completely invisible, and hence, not reachable from VMs outside of a deployment or virtual network (unless configured to be visible via public IP addresses).    * Customer environments are open only through the ports they specify for public access; if the VM is defined to have a public IP address, then all ports are open for public access. |
| **Q. 234:**  CS-3.8 | *Do you design, develop, and deploy multi-tenant applications, systems, and components such that client content and data is appropriately segmented?* | X |  |  | Azure employs a defense-in-depth strategy for boundary protection, including secure segmentation of network environments through several methods including VLANs, ACL restrictions and encrypted communications for remote connectivity. |
| **Q. 235:**  CS-3.9 | *Do you use secure and encrypted channels when migrating physical servers, applications, and content data to/from virtual servers?* | X |  |  | Internal Azure diagrams clearly define boundaries and data flows between zones having different data classification, trust levels or compliance and regulatory requirements.  Communication channels are logically or physically isolated from other networks. Customer information is encrypted during transmission over external networks. Customer configuration information (e.g. connection strings, application settings) supplied through the management portal is protected while in transit and at rest.  Network filtering is implemented to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted platform components. The Microsoft Azure network is segregated to separate customer traffic from management traffic. In addition, SQL Database services include TDS gateways that control information flows through stateful inspection. |
| **Q. 236:**  CS-3.10 | *"Do you have a process for identifying network-based attacks associated with unusual ingress/egress traffic patterns (e.g., MAC spoofing, ARP poising attacks, and/or DDOS attacks)?*  *If yes, what techniques are used? "* | X |  |  | Applies to:   * Deep packet analysis * Traffic throttling * Black-holing * Other:   Microsoft Azure has implemented load balancers and traffic filters to control the flow of external traffic to Microsoft Azure components. Additionally, Microsoft Azure has established automated controls to monitor and detect internally initiated Denial of Service attacks.  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 penetration-testing. Azure’s DDoS defense system is designed to not only withstand attacks from the outside, but also from other Azure tenants:   1. **Network-layer high volume attacks.** These attacks choke network pipes and packet processing capabilities by flooding the network with packets. 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. 2. **Application-layer attacks.** These attacks can be launched against a customer VM. Azure does not provide mitigation or actively block network traffic affecting individual customer deployments, because the infrastructure does not interpret the expected behavior of customer applications. In this case, similar to on-premises deployments, mitigations include:    * Running multiple VM instances behind a load-balanced Public IP address.    * Using firewall proxy devices such as Web Application Firewalls (WAFs) that terminate and forward traffic to endpoints running in a VM. This provides some protection against a broad range of DoS and other attacks, such as low-rate, HTTP, and other application-layer threats. Some virtualized solutions, such as Barracuda Networks, are available that perform both intrusion detection and prevention.    * Web Server add-ons that protect against certain DoS attacks.    * Network ACLs and Security Groups, which can prevent packets from certain IP addresses from reaching VMs.   If a customer determines that their application is under attack, they should contact Azure Customer Support immediately to receive assistance. Azure Customer Support personnel prioritizes these types of requests. |
| **Q. 237:**  CS-3.11 | *Do you have the following procedures and processes for securing virtualized environments?* | X |  |  | Applies to:   * Restricting and monitoring use of utilities that can manage virtual partitions * A system to detect and block attacks targeting virtual infrastructure (e.g., shimming, blue pill, hyper jumping) * Change control of the virtual environment * Restricting hypervisor management or administrative functions based on least privilege * Capability to uniquely identify virtual machines via policy tags or metadata * Other:   Each OS (Host OS, Guest OS, Native OS) is deployed via a “Base Image”. The base image is constructed through a formal build process. Each base image is built upon an OS version in which the kernel, and many other core components, have been modified and optimized to support the Azure environment.  The Host OS and Native OS are hardened operating system images that run on compute (runs as first VM on the node) and storage nodes, and host the Fabric Agent. This has the benefit of reducing the surface area exposed by APIs or unused components. This reduced-footprint operating system includes only those components necessary to the Azure environment, which both improves performance and reduces the potential attack surface.  The baseline configuration lifecycle defines a repeatable process by which baselines are established, evolved and monitored. Five distinct stages create a framework for managing the lifecycle of a baseline: establish and update, implementation (adoption and deployment), scan, reporting, review and analysis.  These processes also apply to Web and Worker roles in Azure Cloud Services, as well as OS gallery images. Customers are responsible for managing virtual machines running as IaaS within their tenant environment. |

# 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](mailto:secure@microsoft.com).
* Service Trust Portal
  + <https://www.microsoft.com/en-us/TrustCenter/STP/default.aspx>