MERIDIA INTERACTIVE SOLUTIONS
1646 West Chester Pike, Suite 15, West Chester, PA 19382
Phone: 610-260-6800, Fax: 610-260-6810, Email: rsvp@meridiaars.com

Photo Communications Corp. DBA Meridia Audience Response

CloudVOTE Standard Response to Physical Security Procedures and Information Security Standards

Last Update: 12/09/16

1646 West Chester Pike, Suite 15, West Chester, PA 19382
Phone: 610-260-6800, Fax: 610-260-6810, Email: rsvp@meridiaars.com

Table of Contents

MERIDIA INTERACTIVE SOLUTIONS
1646 West Chester Pike, Suite 15, West Chester, PA 19382
Phone: 610-260-6800, Fax: 610-260-6810, Email: rsvp@meridiaars.com

Windows Azure Response in the Context of CSA Cloud Control Matrix (*Controls FS-01 through FS-02)*

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
FS-01 **Facility Security - Policy**	Policies and procedures shall be established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas.	Access to all Microsoft buildings is controlled, and access is restricted to those with card reader (swiping the card reader with an authorized ID badge) or biometrics for entry into Data Centers. Front desk personnel are required to positively identify Full-Time Employees (FTEs) or authorized Contractors without ID cards. Staff must wear identity badges at all times, and are required to challenge or report individuals without badges. All guests are required to wear guest badges and be escorted by authorized Microsoft personnel. "Securing offices, rooms, and facilities" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 9.1.3. For more information review of the publicly available ISO standards we are certified against is suggested.
FS-02 **Facility Security - User Access**	Physical access to information assets and functions by users and support personnel shall be restricted.	Access is restricted by job function so that only essential personnel receive authorization to manage Windows Azure services. Physical access authorization utilizes multiple authentication and security processes: badge and smartcard, biometric scanners, on-premises security officers, continuous video surveillance, and two-factor authentication for physical access to the data center environment. In addition to the physical entry controls that are installed on various doors within the data center, the Microsoft Data Center Management organization has implemented operational procedures to restrict physical access to authorized employees, contractors and visitors: • Authorization to grant temporary or permanent access to Microsoft data centers is limited to authorized staff. The requests and corresponding authorization decisions are tracked using a ticketing/access system. • Badges are issued to personnel requiring access after verification of identification. • The Microsoft Data Center Management organization performs a regular access list review. As a result of this audit, the appropriate actions are taken after the review. "Physical and environmental security" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 9. For more information review of the publicly available ISO standards we are certified against is suggested.

Windows Azure Response in the Context of CSA Cloud Control Matrix (*Controls FS-03 through FS-05)*

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
FS-03 **Facility Security - Controlled Access Points**	Physical security perimeters (fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) shall be implemented to safeguard sensitive data and information systems.	Data center buildings are nondescript and do not advertise that Microsoft Data Center hosting services are provided at the location. Access to the data center 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 Data Center that contain critical systems (servers, generators, electrical panels, network equipment, etc.) are either restricted through various security mechanisms such as electronic card access control, keyed lock, ant tailgating and/or biometric devices. "Physical security perimeter and environmental security" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 9. For more information review of the publicly available ISO standards we are certified against is suggested.
FS-04 **Facility Security - Secure Area Authorization**	Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.	"Public access, delivery, loading area and physical/environmental security" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 9. For more information review of the publicly available ISO standards we are certified against is suggested. For additional information also see FS-03
FS-05 **Facility Security - Unauthorized Persons Entry**	Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to percent unauthorized data corruption, compromise and loss.	"Public access, delivery, loading area and physical/environmental security" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 9. For more information review of the publicly available ISO standards we are certified against is suggested. For additional information also see FS-03

Windows Azure Response in the Context of CSA Cloud Control Matrix (*Controls FS-06 through FS-08)*

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
FS-06 **Facility Security - Off-Site Authorization**	Authorization must be obtained prior to relocation or transfer of hardware, software or data to an offsite premises.	Microsoft asset and data protection procedures provide prescriptive guidance around the protection of logical and physical data and include instructions addressing relocation. Customers control where their data is stored. For additional details, see our Privacy Statement available at: http://www.microsoft.com/windowsazure/legal/. "Removal of Property and change management" is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 9.2.7 and 10.1.2. For more information review of the publicly available ISO standards we are certified against is suggested.
FS-07 **Facility Security - Off-Site Equipment**	Policies and procedures shall be established for securing and asset management for the use and secure disposal of equipment maintained and used outside the organization's premise.	Microsoft's asset management policy and acceptable use standards were developed and implemented for Windows Azure technology assets, infrastructure components and services technologies. A customer facing version of the Information Security Policy can be made available upon request. Customers and prospective customers must have a signed NDA or equivalent in order to receive a copy of the Information Security Policy. "Security of equipment off-premises" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 9.2.5. For more information review of the publicly available ISO standards we are certified against is suggested.
FS-08 **Facility Security - Asset Management**	A complete inventory of critical assets shall be maintained with ownership defined and documented.	Windows Azure has implemented a formal policy that requires assets used to provide Windows Azure services to be accounted for and have a designated asset owner. An inventory of major hardware assets in the Windows Azure environment is maintained. Asset owners are responsible for maintaining up-to-date information regarding their assets within the asset inventory including owner or any associated agent, location, and security classification. Asset owners are also responsible for classifying and maintaining the protection of their assets in accordance with the standards. Regular audits occur to verify inventory. "Asset management" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 7. For more information review of the publicly available ISO standards we are certified against is suggested.

Windows Azure Response in the Context of CSA Cloud Control Matrix (*Controls IS-01 through IS-02*)

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
IS-01 **Information Security - Management Program**	An Information Security Management Program (ISMP) has been developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program should address, but not be limited to, the following areas insofar as they relate to the characteristics of the business: • Risk management • Security policy • Organization of information security • Asset management • Human resources security • Physical and environmental security • Communications and operations management • Access control • Information systems acquisition, development, and maintenance	An overall ISMS for Windows Azure has been designed and implemented to address industry best practices around security and privacy. A customer facing version of the Information Security Policy can be made available upon request. Customers and prospective customers must have a signed NDA or equivalent in order to receive a copy of the Information Security Policy. “Establishing and managing the ISMS and Organization of information security” is covered under the ISO 27001 standards, specifically addressed in Clause 4.2 and Annex A, domain 6. For more information review of the publicly available ISO standards we are certified against is suggested.
IS-02 **Information Security - Management Support / Involvement**	Executive and line management shall take formal action to support information security through clear documented direction, commitment, explicit assignment and verification of assignment execution	Each management-endorsed version of the Information Security Policy and all subsequent updates are distributed to all relevant stakeholders. The Information Security Policy is made available to all new and existing Windows Azure employees for review. All Windows Azure employees represent that they have reviewed, and agree to adhere to, all policies within the Information Security Policy documents. All Windows Azure Contractor Staff agree to adhere to the relevant policies within the Information Security Policy. A customer facing version of the Information Security Policy can be made available upon request. Customers and prospective customers must have a signed NDA or equivalent in order to receive a copy of the Information Security Policy. “Management commitment to information security and management responsibility” is covered under the ISO 27001 standards, specifically addressed in Clause 5 and Annex A, domain 6.1.1. For more information review of the publicly available ISO standards we are certified against is suggested.

Windows Azure Response in the Context of CSA Cloud Control Matrix (*Control IS-03 through IS-05)*

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
IS-03 **Information Security - Policy**	Management shall approve a formal information security policy document which shall be communicated and published to employees, contractors and other relevant external parties. The Information Security Policy shall establish the direction of the organization and align to best practices, regulatory, federal/state and international laws where applicable. The Information Security policy shall be supported by a strategic plan and a security program with well-defined roles and responsibilities for leadership and officer roles.	For more information see IS-02 "Information security policy document" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 5.1.1, for more information review of the publicly available ISO standards we are certified against is suggested.
IS-04 **Information Security - Baseline Requirements**	Baseline security requirements shall be established and applied to the design and implementation of (developed or purchased) applications, databases, systems, and network infrastructure and information processing that comply with policies, standards and applicable regulatory requirements. Compliance with security baseline requirements must be reassessed at least annually or upon significant changes.	As part of the overall ISMS framework baseline security requirements are constantly being reviewed, improved and implemented. "Information systems acquisition, development maintenance and security requirements of information systems" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 12. For more information review of the publicly available ISO standards we are certified against is suggested.
IS-05 **Information Security - Policy Reviews**	Management shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing effectiveness and accuracy.	The Windows Azure Information Security Policy undergoes a formal review and update process at a regularly scheduled interval not to exceed 1 year. In the event a significant change is required in the security requirements, it may be reviewed and updated outside of the regular schedule. "Review of the information security policy" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 5.1.2. For more information review of the publicly available ISO standards we are certified against is suggested.

Windows Azure Response in the Context of CSA Cloud Control Matrix (*Controls IS-06 through IS-07)*

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
IS-06 **Information Security - Policy Enforcement**	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation and stated as such in the policies and procedures.	Windows Azure services staff suspected of committing breaches of security and/or violating the Information Security Policy equivalent to a Microsoft Code of Conduct violation are subject to an investigation process and appropriate disciplinary action up to and including termination. Contracting staff suspected of committing breaches of security and/or violations of the Information Security Policy are subject to formal investigation and action appropriate to the associated contract, which may include termination of such contracts. Human Resources is responsible for coordinating disciplinary response. “Information security awareness, education, training and disciplinary process” is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 8.2.2 and 8.2.3. For more information review of the publicly available ISO standards we are certified against is suggested.
IS-07 **Information Security - User Access Policy**	User access policies and procedures shall be documented, approved and implemented for granting and revoking normal and privileged access to applications, databases, and server and network infrastructure in accordance with business, security, compliance and service level agreement (SLA) requirements.	Windows Azure has adopted applicable corporate and organizational security policies, including an Information Security Policy. The policies have been approved, published and communicated to Windows Azure. The Information Security Policy requires that access to Windows Azure assets to be granted based on business justification, with the asset owner's authorization and limited based on "need-to-know" and "least-privilege" principles. In addition, the policy also addresses requirements for access management lifecycle including access provisioning, authentication, access authorization, removal of access rights and periodic access reviews. “Access control” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 11. For more information review of the publicly available ISO standards we are certified against is suggested.

Windows Azure Response in the Context of CSA Cloud Control Matrix (*Controls IS-08 through IS-09)*

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
IS-08 **Information Security - User Access Restriction / Authorization**	Normal and privileged user access to applications, systems, databases, network configurations, and sensitive data and functions shall be restricted and approved by management prior to access granted.	Windows Azure has adopted applicable corporate and organizational security policies, including an Information Security Policy. The policies have been approved, published and communicated to Windows Azure personnel. The Information Security Policy requires that access to Windows Azure assets to be granted based on business justification, with the asset owner's authorization and limited based on "need-to-know" and "least-privilege" principles. In addition, the policy also addresses requirements for access management lifecycle including access provisioning, authentication, access authorization, removal of access rights and periodic access reviews. "User access management and privilege management" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 11.2. For more information review of the publicly available ISO standards we are certified against is suggested.
IS-09 **Information Security - User Access Revocation**	Timely de-provisioning, revocation or modification of user access to the organizations systems, information assets and data shall be implemented upon any change in status of employees, contractors, customers, business partners or third parties. Any change in status is intended to include termination of employment, contract or agreement, change of employment or transfer within the organization.	Managers, owners of applications and data are responsible for reviewing who has access on a periodic basis. Regular access review audits occur to validate appropriate access provisioning has occurred. In Windows Azure environment, Customers are responsible for managing access to the applications customers host on Windows Azure. "Removal of access rights" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 8.3.3. For more information review of the publicly available ISO standards we are certified against is suggested.

Windows Azure Response in the Context of CSA Cloud Control Matrix (*Controls IS-10 through IS-11)*

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
IS-10 **Information Security - User Access Reviews**	All levels of user access shall be reviewed by management at planned intervals and documented. For access violations identified, remediation must follow documented access control policies and procedures.	The Information Security Policy requires that access to Windows Azure assets to be granted based on business justification, with the asset owner's authorization and limited based on "need-to-know" and "least-privilege" principles. In addition, the policy also addresses requirements for access management lifecycle including access provisioning, authentication, access authorization, removal of access rights and periodic access reviews. Managers and owners of applications and data are responsible for reviewing who has access on a periodic basis. Customers control access by their own users and are responsible for ensuring appropriate review of such access. Windows Azure customers register for the service by creating a subscription through the Windows Azure Portal web site. Customers manage applications and storage through their subscription using the Windows Azure management portal. “User access management and privilege management” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 11.2. For more information review of the publicly available ISO standards we are certified against is suggested.
IS-11 **Information Security - Training / Awareness**	A security awareness training program shall be established for all contractors, third party users and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, process and policies, relating to their function relative to the organization.	All appropriate Microsoft staff take part in a Windows Azure and/or GFS 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. All Windows Azure and/or GFS staff are required to take training determined to be appropriate to the services being provided and the role they perform. “Information security awareness, education and training” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 8.2. For more information review of the publicly available ISO standards we are certified against is suggested.

Windows Azure Response in the Context of CSA Cloud Control Matrix (*Controls IS-12 through IS-14)*

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
IS-12 **Information Security - Industry Knowledge / Benchmarking**	Industry security knowledge and benchmarking through networking, specialist security forums, and professional associations shall be maintained.	Microsoft is a member of several industry organizations and both attends and provides speakers to such events and organizations. Microsoft additionally holds several internal trainings. "Contact with special interest groups" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 6.1.7. For more information review of the publicly available ISO standards we are certified against is suggested.
IS-13 **Information Security - Roles/ Responsibilities**	Roles and responsibilities of contractors, employees and third party users shall be documented as they relate to information assets and security.	The Information Security Policy exists in order to provide Windows Azure Staff and Contractor Staff with a current set of clear and concise Information Security Policies including their roles and responsibilities related to information assets and security. These policies provide direction for the appropriate protection of Windows Azure. The Information Security Policy has been created as a component of an overall Information Security Management System (ISMS) for the Windows Azure. The Policy has been reviewed, approved, and is endorsed by Windows Azure management. "Roles and responsibilities of contractors, employees and third party users" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 8.1. For more information review of the publicly available ISO standards we are certified against is suggested.
IS-14 **Information Security - Management Oversight**	Managers are responsible for maintaining awareness of and complying with security policies, procedures and standards that are relevant to their area of responsibility.	Each management-endorsed version of the Information Security Policy and all subsequent updates are distributed to all relevant stakeholders. The Information Security Policy is made available to all new and existing Staff for review. All Windows Azure Staff represent that they have reviewed, and agree to adhere to, all policies within the Policy documents. All Windows Azure Contractor Staff agree to adhere to the relevant policies within the Policy. Should one of these parties not have access to this policy for any reason, the supervising Microsoft agent is responsible for distributing the policy to them. "Management responsibility and management commitment to information security and responsibilities" is covered under the ISO 27001 standards, specifically addressed in Clause 5 and Annex A, domain 6.1. For more information review of the publicly available ISO standards we are certified against is suggested.

Windows Azure Response in the Context of CSA Cloud Control Matrix (*Controls IS-15 through IS-17)*

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
IS-15 **Information Security - Segregation of Duties**	Policies, process and procedures shall be implemented to enforce and assure proper segregation of duties. In those events where user-role conflict of interest constraint exists, technical controls shall be in place to mitigate any risks arising from unauthorized or unintentional modification or misuse of the organization's information assets.	Segregation of duties is established on critical functions within the Windows Azure environment to minimize the risk of unintentional or unauthorized access or change to production systems. Duties and responsibilities are segregated and defined between Windows Azure operation teams. Asset owners/custodians approve different accesses and privileges in the production environment. Segregation of duties is implemented in Windows Azures' environments in order to minimize the potential of fraud, misuse, or error "Segregation of duties" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 10.1.3. For more information review of the publicly available ISO standards we are certified against is suggested.
IS-16 **Information Security - User Responsibility**	Users shall be made aware of their responsibilities for: • Maintaining awareness and compliance with published security policies, procedures, standards and applicable regulatory requirements • Maintaining a safe and secure working environment • Leaving unattended equipment in a secure manner	All appropriate Microsoft employees take part in a Windows Azure and/or GFS security-training program, and are recipients of periodic security awareness updates when applicable. Security education is an on-going process and is conducted at minimum annually in order to minimize risks. All appropriate Windows Azure and GFS contractor staff are required to take any training determined to be appropriate to the services being provided and the role they perform. "User responsibilities" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 11.3. For more information review of the publicly available ISO standards we are certified against is suggested.
IS-17 **Information Security Workspace**	Policies and procedures shall be established for clearing visible documents containing sensitive data when a workspace is unattended and enforcement of workstation session logout for a period of inactivity.	Technical and procedurals controls are part of Microsoft's policies including areas such as defined session time-out requirements. "User responsibilities" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 11.3. For more information review of the publicly available ISO standards we are certified against is suggested.

Windows Azure Response in the Context of CSA Cloud Control Matrix (*Controls IS-18 through IS-19)*

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
IS-18 **Information Security - Encryption**	Policies and procedures shall be established and mechanisms implemented for encrypting sensitive data in storage (e.g., file servers, databases, and end-user workstations) and data in transmission (e.g., system interfaces, over public networks, and electronic messaging).	Microsoft restricts access to customer data. Customer may implement encryption of customer data within the customer's application. Customers may encrypt data stored in XStore. 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. "Exchange of information" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 10.8. For more information review of the publicly available ISO standards we are certified against is suggested.
IS-19 **Information Security - Encryption Key Management**	Policies and procedures shall be established and mechanisms implemented for effective key management to support encryption of data in storage and in transmission.	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 Windows Azure service. "Media Handling" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 12.3.2. For more information review of the publicly available ISO standards we are certified against is suggested.

Windows Azure Response in the Context of CSA Cloud Control Matrix (*Control IS-20)*

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
IS-20 **Information Security - Vulnerability / Patch Management**	Policies and procedures shall be established and mechanism implemented for vulnerability and patch management, ensuring that application, system, and network device vulnerabilities are evaluated and Contractor-supplied security patches applied in a timely manner taking a risk-based approach for prioritizing critical patches.	Windows Azure component teams get notifications of potential vulnerabilities and the latest software updates from the Microsoft Security Response Center (MSRC) and GFS. The component teams analyze software updates relevance to Windows Azure production environment and review the associated vulnerabilities based on their criticality. Software updates are released through the monthly OS release cycle using change and release management procedures. Emergency out-of-band security software updates (0-day & Software Security Incident Response Process - SSIRP updates) are deployed as quickly as possible. If customers use the default "Auto Upgrade" option, software updates will be applied their VMs automatically. Otherwise, customers have the option to upgrade to the latest OS image through the portal. In case of a VM role, customers are responsible for evaluating and updating their VMs. Microsoft's Security Response Center (MSRC) regularly monitors external security vulnerability awareness sites. As part of the routine vulnerability management process, Windows Azure evaluates our exposure to these vulnerabilities and leads action across Microsoft Server and Tools Business (STB) to mitigate risks when necessary. "Control of technical vulnerabilities" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 12.6. For more information review of the publicly available ISO standards we are certified against is suggested.

Windows Azure Response in the Context of CSA Cloud Control Matrix (*Controls IS-21 through IS-22)*

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
IS-21 **Information Security - Anti-Virus / Malicious Software**	Ensure that all antivirus programs are capable of detecting, removing, and protecting against all known types of malicious or unauthorized software with antivirus signature updates at least every 12 hours.	The Windows Azure Security group responds to malicious events, including escalating and engaging specialized support groups. A number of key security parameters are monitored to identify potentially malicious activity on the systems. "Protection against malicious code" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 10.4. For more information review of the publicly available ISO standards we are certified against is suggested.
IS-22 **Information Security - Incident Management**	Policy, process and procedures shall be established to triage security related events and ensure timely and thorough incident management.	Incident handling, management roles and responsibilities have been defined for the Incident Engineer, Incident Manager, Communication Manager and the Feature teams. Windows Azure Operations Managers are responsible for overseeing investigation and resolution of security and privacy incidents with support from other functions. Processes for escalating and engaging other functions for investigating and analyzing incidents are established. An escalation and communication plan to notify Privacy, Legal or Executive Management in the event of a security incident has been established. Our process consists of the following steps: Identification, containment, eradication, recovery, and lessons learned. "Security incident response plans" are covered under the ISO 27001 standards, specifically addressed in Annex A, domain 13.2. For more information review of the publicly available ISO standards we are certified against is suggested.

Windows Azure Response in the Context of CSA Cloud Control Matrix (*Control IS-23)*

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
IS-23 **Information Security - Incident Reporting**	Contractors, employees and third party users shall be made aware of their responsibility to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a prompt and expedient manner in compliance with statutory, regulatory and contractual requirements.	Windows Azure has developed robust processes to facilitate a coordinated response to incidents if one was to occur. A security event may include, among other things unauthorized access resulting in loss, disclosure or alteration of data. The Windows Azure Incident Response process follows the following phases: • Identification – System and security alerts may be harvested, correlated, and analyzed. Events are investigated by Microsoft operational and security organizations. If an event indicates a security issue, the incident is assigned a severity classification and appropriately escalated within Microsoft. This escalation will include product, security, and engineering specialists. • Containment – The escalation team evaluates the scope and impact of an incident. The immediate priority of the escalation team is to ensure the incident is contained and data is safe. The escalation team forms the response, performs appropriate testing, and implements changes. In the case where in-depth investigation is required, content is collected from the subject systems using best-of-breed forensic software and industry best practices. • Eradication – After the situation is contained, the escalation team moves toward eradicating any damage caused by the security breach, and identifies the root cause for why the security issue occurred. If vulnerability is determined, the escalation team reports the issue to product engineering. • Recovery – During recovery, software or configuration updates are applied to the system and services are returned to a full working capacity. • Lessons Learned – Each security incident is analyzed to ensure the appropriate mitigations applied to protect against future reoccurrence. If Windows Azure personnel determine that a customer's data was breached or otherwise subject to unauthorized access, the customer will be notified. "Reporting security weaknesses and responsibilities and procedures" is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 13.1.2 and 13.2. For more information review of the publicly available ISO standards we are certified against is suggested.

Windows Azure Response in the Context of CSA Cloud Control Matrix (*Controls IS-24 through IS-26)*

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
IS-24 **Information Security - Incident Response Legal Preparation**	In the event a follow-up action concerning a person or organization after an information security incident requires legal action proper forensic procedures including chain of custody shall be required for collection, retention, and presentation of evidence to support potential legal action subject to the relevant jurisdiction.	As part of the 'containment' step in our Security Incident Response Process, the immediate priority of the escalation team is to ensure the incident is contained and data is safe. The escalation team forms the response, performs appropriate testing, and implements changes. "Security incident response plans and collection of evidence" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 13.2. For more information review of the publicly available ISO standards we are certified against is suggested.
IS-25 **Information Security - Incident Response Metrics**	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.	Information security incidents are classified into severity levels and processed according to the severity level. Regular reporting of incidents is carried out for management reporting. "Management information security incidents and learning from information security incidents" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 13.2. For more information review of the publicly available ISO standards we are certified against is suggested.
IS-26 **Information Security - Acceptable Use**	Policies and procedures shall be established for the acceptable use of information assets.	Customer Data will be used only to provide customer the Windows Azure service. This may include troubleshooting aimed at preventing, detecting and repairing problems affecting the operation of the services and the improvement of features that involve the detection of, and protection against, emerging and evolving threats to the user (such as malware or spam). More information on Microsoft's commitment around use of customer data can be found in the Privacy Statement and Online Services Use Rights available at: http://www.microsoft.com/windowsazure/legal/. "Acceptable use" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 7.1.3. For more information review of the publicly available ISO standards we are certified against is suggested.

Windows Azure Response in the Context of CSA Cloud Control Matrix (*Controls IS-27 through IS-29)*

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
IS-27 **Information Security - Asset Returns**	Employees, contractors and third party users must return all assets owned by the organization within a defined and documented time frame once the employment, contract or agreement has been terminated.	Employees, contractors and third party users are formally notified to destroy or return, as applicable, any physical materials that Microsoft has provided to them during the term of employment or the period of Contractor agreement and any electronic media must be removed from Contractor or third party infrastructure. Microsoft may also conduct an audit to make sure data is removed in an appropriate manner. "Return of assets" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 8.3.2. For more information review of the publicly available ISO standards we are certified against is suggested.
IS-28 **Information Security - eCommerce Transactions**	Electronic commerce (e-commerce) related data traversing public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure or modification in such a manner to prevent contract dispute and compromise of data.	Windows Azure does not provide e-commerce solutions.
IS-29 **Information Security - Audit Tools Access**	Access to, and use of, audit tools that interact with the organizations information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.	Access to information systems audit tools are restricted to authorized personnel within Windows Azure. A delegated management model enables administrators to have only the access they need to perform specific tasks, reducing the potential for error and allowing access to systems and functions strictly on an as-needed basis. Windows Azure has formal monitoring processes to include frequency of review for Standard Operating Procedures and review oversight processes and procedures. "Protection of information systems audit tools and protection of log information" is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 15.3.2 and 10.10.3. For more information review of the publicly available ISO standards we are certified against is suggested.

Windows Azure Response in the Context of CSA Cloud Control Matrix (*Controls IS-30 through IS-31)*

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
IS-30 **Information Security - Diagnostic / Configuration Ports Access**	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	Access control policy is a component of overall policies and undergoes a formal review and update process. Access to Windows Azures' assets is granted based upon business requirements and with the asset owner's authorization. Additionally: • Access to assets is granted based upon need-to-know and least-privilege principles. • Where feasible, role-based access controls are used to allocate logical access to a specific job function or area of responsibility, rather than to an individual. • Physical and logical access control policies are consistent with standards. Windows Azure controls physical access to diagnostic and configuration ports through physical data center controls. Diagnostic and configuration ports are only accessible by arrangement between service/asset owner and hardware/software support personnel requiring access. Ports, services, and similar facilities installed on a computer or network facility, which are not specifically required for business functionality, are disabled or removed. "Network controls access controls" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 10.6.1, 11.1.1, and 11.4.4. For more information review of the publicly available ISO standards we are certified against is suggested.
IS-31 **Information Security - Network / Infrastructure Services**	Network and infrastructure service level agreements (in-house or outsourced) shall clearly document security controls, capacity and service levels, and business or customer requirements.	Capacity management: Proactive monitoring continuously measures the performance of key subsystems of the Windows Azure services platform against the established boundaries for acceptable service performance and availability. When a threshold is reached or an irregular event occurs, the monitoring system generates warnings so that operations staff can address the threshold or event. System performance and capacity utilization is proactively planned to optimize the environment. The main underlying network infrastructure is currently managed by GFS. SLAs to service providers or equipment manufacturers are qualified by GFS's ISO 27001 certification. "Addressing security in third party agreements and security of network services" is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 6.2.3 and 10.6.2. For more information review of the publicly available ISO standards we are certified against is suggested.

Windows Azure Response in the Context of CSA Cloud Control Matrix (*Controls IS-32 through LG-01)*

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
IS-32 **Information Security - Portable / Mobile Devices**	Policies and procedures shall be established and measures implemented to strictly limit access to sensitive data from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDAs), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization's facilities).	Windows Azure teams and personnel are required to adhere to applicable policies, which do not permit mobile computing devices to the production environment, unless those devices have been approved for use by Windows Azure Management. Mobile computing access points are required to adhere with the wireless device security requirements. "Access control to mobile computing and communications" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 11.7.1. For more information review of the publicly available ISO standards we are certified against is suggested.
IS-33 **Information Security - Source Code Access Restriction**	Access to application, program or object source code shall be restricted to authorized personnel on a need to know basis. Records shall be maintained regarding the individual granted access, reason for access and version of source code exposed.	Windows Azure source code libraries are limited to authorized personnel. Where feasible, source code libraries maintain separate project work spaces for independent projects. Windows Azure and Windows Azure Contractors are granted access only to those work spaces which they need access to perform their duties. Source code libraries enforce control over changes to source code by requiring a review from designated reviewers prior to submission. An audit log detailing modifications to the source code library is maintained. "Access control and access control to program source code" is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 11 and 12.4.3. For more information review of the publicly available ISO standards we are certified against is suggested.
IS-34 **Information Security - Utility Programs Access**	Utility programs capable of potentially overriding system, object, network, virtual machine and application controls shall be restricted.	Utility programs undergo changes and the release management process and are restricted to authorized personnel only. "User authentication for external connections" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 11.4.2. For more information, review of the publically available ISO standards we are certified against is suggested.
LG-01 **Legal - Non-Disclosure Agreements**	Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented and reviewed at planned intervals.	Microsoft Legal and Human Resources maintain policies and procedures defining the implementation and execution of non- disclosure and confidentiality agreements. "Confidentiality agreements and non-disclosure agreements" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 6.1.5. For more information review of the publicly available ISO standards we are certified against is suggested.