ArcGIS Online
Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) Answers
August 2015 – Version 1.4

Attached are Esri's self-assessment answers to the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) for ArcGIS Online. The questionnaire published by the CSA, provides a way to reference and document what security controls exist in Esri's ArcGIS Online offering. The questionnaire provides a set of 98 questions a cloud consumer and cloud auditor may wish to ask of a cloud provider.

The CSA is a "not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing" (https://cloudsecurityalliance.org/about/). A wide range of industry security practitioners, corporations, and associations participate in this organization to achieve its mission. Esri has been providing answers for version 1.4 of the CSA CCM since 2013, and will update this document focused on ArcGIS Online for newer CCM revisions in the future.

ArcGIS Online was granted a Federal Information Security Management Act (FISMA) Low Authority to Operate (ATO) by the United States Department of Agriculture (USDA) in 2014. Customers desiring alignment with the accreditation can use ArcGIS Online to host scalable tile services for broad public dissemination, while leveraging their own agency accredited infrastructure feature services for hosting more sensitive information. For more information concerning the security, privacy and compliance of ArcGIS Online please see http://Trust.ArcGIS.com

ArcGIS Online utilizes the World-Class Cloud Infrastructure of Microsoft Azure and Amazon Web Services, both of which have completed the CSA questionnaires for their capabilities and may be downloaded from the CSA Registry located at: https://cloudsecurityalliance.org/star/#_registry

The latest version of the ArcGIS Online CSA answers will be available at the following location until further notice: http://downloads.esri.com/resources/enterprisegis/AGOL_CSA_CCM.pdf

For any questions/concerns/feedback please contact the Esri Security Standards and Architecture Team at:
SecureSoftwareServices@esri.com

ArcGIS Online Cloud Controls Matrix (CCM) Answers

Control Area	Control ID	Control Specification	ArcGIS Online Response	Scope Applicability	
				ISO/IEC 27001-2005	NIST 800-53 R3
Compliance - Audit Planning	CO-01	Audit plans, activities and operational action items focusing on data duplication, access, and data boundary limitations shall be designed to minimize the risk of business process disruption. Audit activities must be planned and agreed upon in advance by stakeholders.	ArcGIS Online is audited in accordance with FISMA Low requirements. ArcGIS Online utilizes cloud infrastructure from MS Azure, and Amazon Web Services. Each of the cloud infrastructure providers regularly audit their operations and can provide them under their own NDA's.	Clause 4.2.3 e) Clause 4.2.3b Clause 5.1 g Clause 6 A.15.3.1	CA-2 CA-7 PL-6
Compliance - Independent Audits	CO-02	Independent reviews and assessments shall be performed at least annually, or at planned intervals, to ensure the organization is compliant with policies, procedures, standards and applicable regulatory requirements (i.e., internal/external audits, certifications, vulnerability and penetration testing)	ArcGIS Online utilizes third party auditors as part of FISMA Low compliance. Continuous monitoring includes vulnerability assessments and security control reviews. For security and operational reasons, Esri does not allow our customers to perform their own audits on ArcGIS Online as stated in the Terms of Service. Customers may also obtain cloud infrastructure provider reports and certifications directly from the vendors of Microsoft Azure and Amazon Web Services.	Clause 4.2.3e Clause 5.1 g Clause 5.2.1 d) Clause 6 A.6.1.8	CA-1 CA-2 CA-6 RA-5
Compliance - Third Party Audits	CO-03	Third party service providers shall demonstrate compliance with information security and confidentiality, service definitions and delivery level agreements included in third party contracts. Third party reports, records and services shall undergo audit and review, at planned intervals, to govern and maintain compliance with the service delivery agreements.	Esri periodically utilizes third party assessors for their products. ArcGIS Online utilizes cloud infrastructure from MS Azure, and Amazon Web Services. Each of the cloud infrastructure providers regularly audit their operations and can provide them under their own NDA's	A.6.2.3 A.10.2.1 A.10.2.2 A.10.6.2	CA-3 SA-9 SA-12 SC-7
Compliance - Contact / Authority Maintenance	CO-04	Liaisons and points of contact with local authorities shall be maintained in accordance with business and customer requirements and compliance with legislative, regulatory, and contractual requirements. Data, objects, applications, infrastructure and hardware may be assigned legislative domain and jurisdiction to facilitate proper compliance points of contact.	Esri maintains contact with external parties such as regulatory bodies, service providers, and industry forums to ensure appropriate action can be quickly taken and advice obtained when necessary.	A.6.1.6 A.6.1.7	AT-5 IR-6 SI-5

ArcGIS Online Cloud Controls Matrix (CCM) Answers

Control Area	Control ID	Control Specification	ArcGIS Online Response	Scope Applicability	
				ISO/IEC 27001-2005	NIST 800-53 R3
Compliance - Information System Regulatory Mapping	CO-05	Statutory, regulatory, and contractual requirements shall be defined for all elements of the information system. The organization's approach to meet known requirements, and adapt to new mandates shall be explicitly defined, documented, and kept up to date for each information system element in the organization. Information system elements may include data, objects, applications, infrastructure and hardware. Each element may be assigned a legislative domain and jurisdiction to facilitate proper compliance mapping.	ArcGIS Online complies with data protection and privacy laws generally applicable to Esri's provision of ArcGIS Online. ArcGIS Online is compliant with FISMA Low requirements which is based on NIST SP 800-53 R3. A mapping of these controls to ISO 27001 is available here: http://downloads.esri.com/resources/enterprisegis/FISMA_Low_ISO_Mapping.pdf The ArcGIS Online Privacy Statement is certified compliant with independant, international, industry-accepted privacy standards including TRUSTe Certified Privacy Seal and EU Safe Harbor. For more information, see: http://doc.arcgis.com/en/trust/privacy/overview.htm Customers retain ownership of their data and are responsible for compliance with laws and regulations specific to their industry or particular use of ArcGIS Online. ArcGIS Online uses Cloud Infrastructure Providers that are compliant with ISO 27001 and FedRAMP Moderate requirements.	Clause 4.2.1 b) 2) Clause 4.2.1 c) 1) Clause 4.2.1 g) Clause 4.2.3 d) 6) Clause 4.3.3 Clause 5.2.1 a - f Clause 7.3 c) 4) A.7.2.1 A.15.1.1 A.15.1.3 A.15.1.4 A.15.1.6	AC-1 AT-1 AU-1 CA-1 CM-1 CP-1 IA-1 IA-7 IR-1 MA-1 MP-1 PE-1 PL-1 PM-1 PS-1 RA-1 RA-2 SA-1 SA-6 SC-1 SC-13 SI-1
Compliance - Intellectual Property	CO-06	Policy, process and procedure shall be established and implemented to safeguard intellectual property and the use of proprietary software within the legislative jurisdiction and contractual constraints governing the organization.	Esri maintains a robust NIST 800-53 aligned set of information security policies and procedures which address the confidentiality of customer data and associated protection mechanisms.	Clause 4.2.1 A.6.1.5 A.7.1.3 A.10.8.2 A.12.4.3 A.15.1.2	SA-6 SA-7 PM-5
Data Governance - Ownership / Stewardship	DG-01	All data shall be designated with stewardship with assigned responsibilities defined, documented and communicated.	Data stored within ArcGIS Online meets FISMA Low categorized requirements. Customers are responsible for implementing workflows to enforce this categorization level. Customers retain full ownership of their data.	A.6.1.3 A.7.1.2 A.15.1.4	CA-2 PM-5 PS-2 RA-2 SA-2

ArcGIS Online Cloud Controls Matrix (CCM) Answers

Control Area	Control ID	Control Specification	ArcGIS Online Response	Scope Applicability	
				ISO/IEC 27001-2005	NIST 800-53 R3
Data Governance - Classification	DG-02	Data, and objects containing data, shall be assigned a classification based on data type, jurisdiction of origin, jurisdiction domiciled, context, legal constraints, contractual constraints, value, sensitivity, criticality to the organization and third party obligation for retention and prevention of unauthorized disclosure or misuse.	Esri classifies data according to the Esri Technology Control Plan and then implements a standard set of Security and Privacy attributes. Esri does not classify data uploaded and stored by customers in ArcGIS Online but treats all Customer Data in accordance with the commitment outlined in CO-06. As stated in the Terms of Services, the following data set classifications shall not be used within ArcGIS Online: International Traffic in Arms Regulations (ITAR), Unclassified Controlled Technical Information (UCTI), and Protected Health Information (PHI).	A.7.2.1	RA-2 AC-4
Data Governance - Handling / Labeling / Security Policy	DG-03	Polices and procedures shall be established for labeling, handling and security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that acts as aggregate containers for data.	ArcGIS Online customers retain ownership of their data and may implement a labeling and handling policy and procedures to meet their requirements.	A.7.2.2 A.10.7.1 A.10.7.3 A.10.8.1	AC-16 MP-1 MP-3 PE-16 SI-12 SC-9
Data Governance - Retention Policy	DG-04	(v1.1) Policies and procedures for data retention and storage shall be established and backup or redundancy mechanisms implemented to ensure compliance with regulatory, statutory, contractual or business requirements. Testing the recovery of backups must be implemented at planned intervals.	Esri backs up ArcGIS Online infrastructure data regularly. Customer data is replicated to redundant infrastructure. ArcGIS Online provides customers with the ability to delete their data; however it is the customer's responsibility to manage data retention to their own requirements. A KBA describing backing up customer data is available at: http://support.esri.com/en/knowledgebase/techarticles/detail/41166 .	Clause 4.3.3 A.10.5.1 A.10.7.3	CP-2 CP-6 CP-7 CP-8 CP-9 SI-12 AU-11

ArcGIS Online Cloud Controls Matrix (CCM) Answers

Control Area	Control ID	Control Specification	ArcGIS Online Response	Scope Applicability	
				ISO/IEC 27001-2005	NIST 800-53 R3
Data Governance - Secure Disposal	DG-05	Policies and procedures shall be established and mechanisms implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.	When a storage device has reached the end of its useful life, ArcGIS Online cloud infrastructure providers procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. The Cloud infrastructure providers use the techniques detailed in DoD 5220.22-M (“National Industrial Security Program Operating Manual “) or NIST 800-88 (“Guidelines for Media Sanitization”) to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry standard practices.	A.9.2.6 A.10.7.2	MP-6 PE-1
Data Governance - Non-Production Data	DG-06	Production data shall not be replicated or used in non-production environments.	ArcGIS Online customers retain ownership of their own data. ArcGIS Online provides customers the ability to maintain and develop production and non-production organization environments. It is the responsibility of the customer to ensure that their production data is not replicated to the non-production environments. Movement or copying of Customer Data by Esri out of the production environment into a non-production environment is prohibited except where customer consent is obtained for troubleshooting the service, or at the directive of Esri's legal department.	A.7.1.3 A.10.1.4 A.12.4.2 A.12.5.1	SA-11 CM-04

ArcGIS Online Cloud Controls Matrix (CCM) Answers

Control Area	Control ID	Control Specification	ArcGIS Online Response	Scope Applicability	
				ISO/IEC 27001-2005	NIST 800-53 R3
Data Governance - Information Leakage	DG-07	Security mechanisms shall be implemented to prevent data leakage.	Physical and logical controls are implemented by cloud infrastructure providers and fully documented. ArcGIS Online feature service data is stored in separate database instances per organization. A separate Data Loss Prevention (DLP) solution has not been deployed for ArcGIS Online. It is recommended that customers do not allow public sharing from their ArcGIS Online organization unless required. This can be configured in the security settings for organization. Finally, customers that have data sensitivity concerns often choose to implement a hybrid implementation with ArcGIS for Server where more sensitive data is kept on-premises. This enables the customer to leverage their existing DLP appliance for those data sets.	A.10.6.2 A.12.5.4	AC-2 AC-3 AC-4 AC-6 AC-11 AU-13 PE-19 SC-28 SA-8 SI-7
Data Governance - Risk Assessments	DG-08	Risk assessments associated with data governance requirements shall be conducted at planned intervals considering the following: • Awareness of where sensitive data is stored and transmitted across applications, databases, servers and network infrastructure • Compliance with defined retention periods and end-of-life disposal requirements • Data classification and protection from unauthorized use, access, loss, destruction, and falsification	ArcGIS Online conducts regular risk assessment as part of alignment with FISMA requirements. ArcGIS Online cloud infrastructure providers publish independent auditor reports and certifications to provide customers with considerable information regarding the policies, processes, and controls established and operated by them.	Clause 4.2.1 c) & g) Clause 4.2.3 d) Clause 4.3.1 & 4.3.3 Clause 7.2 & 7.3 A.7.2 A.15.1.1 A.15.1.3 A.15.1.4	CA-3 RA-2 RA-3 MP-8 PM-9 SI-12
Facility Security - Policy	FS-01	Policies and procedures shall be established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas.	Access to all cloud provider buildings is controlled, and access is restricted to those with card reader 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 cloud provider personnel.	A.5.1.1 A.9.1.3 A.9.1.5	CA-2 PE-1 PE-6 PE-7 PE-8

ArcGIS Online Cloud Controls Matrix (CCM) Answers

Control Area	Control ID	Control Specification	ArcGIS Online Response	Scope Applicability	
				ISO/IEC 27001-2005	NIST 800-53 R3
Facility Security - User Access	FS-02	Physical access to information assets and functions by users and support personnel shall be restricted.	Cloud infrastructure provider access is restricted by job function so that only essential personnel receive authorization to manage cloud infrastructure 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.	A.9.1.1 A.9.1.2	PE-2 PE-3 PE-4 PE-5 PE-6
Facility Security - Controlled Access Points	FS-03	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.	Physical security controls include but are not limited to perimeter controls such as fencing, walls, security staff, video surveillance, intrusion detection systems and other electronic means.	A.9.1.1	PE-2 PE-3 PE-6 PE-18
Facility Security - Secure Area Authorization	FS-04	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 the cloud infrastructure providers are certified against is suggested. For additional information also see FS-03	A.9.1.1 A.9.1.2	PE-2 PE-3 PE-6 PE-7 PE-8 PE-18
Facility Security - Unauthorized Persons Entry	FS-05	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.	Cloud infrastructure provider physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access datacenter floors.	A.9.1.6	PE-7 PE-16 PE-18
Facility Security - Off-Site Authorization	FS-06	Authorization must be obtained prior to relocation or transfer of hardware, software or data to an offsite premises.	All ArcGIS Online customer data resides on United States soil within the confines of the Amazon Web Service US Regions (East, West), and Microsoft Azure US Regions (South Central, East, West). ArcGIS Online customers will be notified if Esri proposes storing any of their data outside US soil.	A.9.2.7 A.10.1.2	MA-1 MA-2 PE-16

ArcGIS Online Cloud Controls Matrix (CCM) Answers

Control Area	Control ID	Control Specification	ArcGIS Online Response	Scope Applicability	
				ISO/IEC 27001-2005	NIST 800-53 R3
Facility Security - Off-Site Equipment	FS-07	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.	ArcGIS Online cloud infrastructure providers have established policies and procedures for addressing off-site equipment aligning with ISO 27001 standards.	A.9.2.5 A.9.2.6	AC-17 MA-1 PE-1 PE-16 PE-17
Facility Security - Asset Management	FS-08	A complete inventory of critical assets shall be maintained with ownership defined and documented.	In alignment with ISO 27001 standards, cloud infrastructure provider hardware assets are assigned an owner, tracked and monitored by their personnel with inventory management tools. The cloud infrastructure procurement and supply chain team maintain relationships with all suppliers.	A.7.1.1 A.7.1.2	CM-8
Human Resources Security - Background Screening	HR-01	Pursuant to local laws, regulations, ethics and contractual constraints all employment candidates, contractors and third parties will be subject to background verification proportional to the data classification to be accessed, the business requirements and acceptable risk.	All ArcGIS Online and cloud infrastructure provider employees are required to complete a standard background check as part of the hiring process. Background checks may include but are not limited to review of information relating to a candidate's education, employment, and criminal history.	A.8.1.2	PS-2 PS-3
Human Resources Security - Employment Agreements	HR-02	(v1.1) Prior to granting individuals physical or logical access to facilities, systems or data, employees, contractors, third party users and tenants and/or customers shall contractually agree and sign equivalent terms and conditions regarding information security responsibilities in employment or service contract.	As part of the ArcGIS Online FISMA accreditation applicable employees must sign a rules of behavior document further enforcing requirements beyond the company employee handbook. Cloud infrastructure providers have their own security training and employee agreements they enforce aligning with ISO 27001 standards.	A.6.1.5 A.8.1.3	PL-4 PS-6 PS-7
Human Resources - Employment Termination	HR-03	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented and communicated.	Esri Human Resources Policy drives employee termination processes for ArcGIS Online.	A.8.3.1	PS-4 PS-5

ArcGIS Online Cloud Controls Matrix (CCM) Answers

Control Area	Control ID	Control Specification	ArcGIS Online Response	Scope Applicability	
				ISO/IEC 27001-2005	NIST 800-53 R3
Information Security - Management Program	IS-01	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	ArcGIS Online's ISMP is based upon NIST standards as part of FISMA accreditation. For international customers, a mapping of FISMA security controls to ISO 27001 controls is available in NIST Special Publication 800-53 , Appendix H available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf Cloud infrastructure providers implement ISO 27001 certified ISMP's.	Clause 4.2 Clause 5 A.6.1.1 A.6.1.2 A.6.1.3 A.6.1.4 A.6.1.5 A.6.1.6 A.6.1.7 A.6.1.8	PM-1 PM-2 PM-3 PM-4 PM-5 PM-6 PM-7 PM-8 PM-9 PM-10 PM-11
Information Security - Management Support / Involvement	IS-02	Executive and line management shall take formal action to support information security through clear documented direction, commitment, explicit assignment and verification of assignment execution	Cloud infrastructure providers ensure policy and procedures are in alignment with ISO 27001 standards. ArcGIS Online security policies and procedures will be signed and reviewed by executive management and disseminated to team members in alignment with the FISMA accreditation.	Clause 5 A.6.1.1	CM-1 PM-1 PM-11

ArcGIS Online Cloud Controls Matrix (CCM) Answers

Control Area	Control ID	Control Specification	ArcGIS Online Response	Scope Applicability	
				ISO/IEC 27001-2005	NIST 800-53 R3
Information Security - Policy	IS-03	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	Clause 4.2.1 Clause 5 A.5.1.1 A.8.2.2	AC-1 AT-1 AU-1 CA-1 CM-1 IA-1 IR-1 MA-1 MP-1 MP-1 PE-1 PL-1 PS-1 SA-1 SC-1 SI-1
Information Security - Baseline Requirements	IS-04	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 FISMA accreditation, baseline security requirements are constantly being reviewed, improved and implemented as part of a Continuous Monitoring Program.	A.12.1.1 A.15.2.2	CM-2 SA-2 SA-4
Information Security - Policy Reviews	IS-05	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.	ArcGIS Online security policies undergo a formal review and update process at a regularly scheduled interval not to exceed 3 years as part of the FISMA continuous assessment and monitoring process. In the event a significant change is required in the security requirements, it may be reviewed and updated outside of the regular schedule.	Clause 4.2.3 f) A.5.1.2	AC-1 AT-1 AU-1 CA-1 CM-1 CP-1 IA-1 IA-5 IR-1 MA-1

ArcGIS Online Cloud Controls Matrix (CCM) Answers

Control Area	Control ID	Control Specification	ArcGIS Online Response	Scope Applicability	
				ISO/IEC 27001-2005	NIST 800-53 R3
Information Security - Policy Enforcement	IS-06	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.	ArcGIS Online and cloud infrastructure employees who violate company standards or protocols are investigated and appropriate disciplinary action (e.g. warning, performance plan, suspension, and/or termination) is followed.	A.8.2.3	PL-4 PS-1 PS-8
Information Security - User Access Policy	IS-07	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.	ArcGIS Online employees adhere to a rules of behavior policy outlining user access. Operations personnel revoke physical and logical access privileges as a component of the termination process.	A.11.1.1 A.11.2.1 A.11.2.4 A.11.4.1 A.11.5.2 A.11.6.1	AC-1 IA-1
Information Security - User Access Restriction / Authorization	IS-08	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.	Less than 10 Esri employees, that are speciallized ArcGIS Online administrators, utilizing X.509 certificates for authentication, have access to customer data.	A.11.2.1 A.11.2.2 A.11.4.1 A 11.4.2 A.11.6.1	AC-3 AC-5 AC-6 IA-2 IA-4 IA-5
Information Security - User Access Revocation	IS-09	Timely deprovisioning, 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.	Customers are responsible for managing access to the applications and services customers host on ArcGIS Online. Customer can choose to use the built-in ArcGIS Online user store or use Enterprise Logins which allows customers to leverage their enterprise AD/LDAP by using an SAML 2.0 compliant Identity Provider (IdP). This would ensure that once a user account is disabled in an organization enterprise user store (AD/LDAP), that user would no longer be able to access ArcGIS Online.	A.8.3.3 A.11.1.1 A.11.2.1 A.11.2.2	AC-2 PS-4 PS-5
Information Security - User Access Reviews	IS-10	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.	In alignment with FISMA requirements, ArcGIS Online system user access, at all levels, is reviewed at least once per quarter. Customers control access by their own users and are responsible for ensuring appropriate review of such access.	A.11.2.4	AC-2 AU-6 PM-10 PS-6 PS-7

ArcGIS Online Cloud Controls Matrix (CCM) Answers

Control Area	Control ID	Control Specification	ArcGIS Online Response	Scope Applicability	
				ISO/IEC 27001-2005	NIST 800-53 R3
Information Security - Training / Awareness	IS-11	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.	Annual security training is provided for ArcGIS Online employees.	Clause 5.2.2 A.8.2.2	AT-1 AT-2 AT-3 AT-4
Information Security - Industry Knowledge / Benchmarking	IS-12	Industry security knowledge and benchmarking through networking, specialist security forums, and professional associations shall be maintained.	Esri and it's cloud infrastructure providers maintain contacts with industry groups and professional services related to security	A.6.1.7	AT-5 SI-5
Information Security - Roles / Responsibilities	IS-13	Roles and responsibilities of contractors, employees and third party users shall be documented as they relate to information assets and security.	ArcGIS Online system administrator roles and responsibilities are documented within the internal ArcGIS Online System Security Plan. End-user roles and responsibilities are documented within the ArcGIS Online application documentation.	Clause 5.1 c) A.6.1.2 A.6.1.3 A.8.1.1	AT-3 PL-4 PM-10 PS-1 PS-6 PS-7
Information Security - Management Oversight	IS-14	Managers are responsible for maintaining awareness of and complying with security policies, procedures and standards that are relevant to their area of responsibility.	Managers of ArcGIS Online employees are responsible for ensuring awareness of applicable security policies and procedures for team members.	Clause 5.2.2 A.8.2.1 A.8.2.2 A 11.2.4 A.15.2.1	AT-2 AT-3 CA-1 CA-5 CA-6 CA-7 PM-10
Information Security - Segregation of Duties	IS-15	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 exist, technical controls shall be in place to mitigate any risks arising from unauthorized or unintentional modification or misuse of the organization's information assets.	Cloud infrastructure providers utilize segregation of duties for critical functional to minimize the risk of unintentional or unauthorized access or change to production systems. Customers retain the ability to manage segregation of duties of their ArcGIS Online organization resources. The use of custom roles within ArcGIS Online enables permissions of specific user groups to be applied with much more granularity than the default roles of Administrator, Publisher, and User. For additional information, see: http://doc.arcgis.com/en/arcgis-online/reference/roles.htm	A.10.1.3	AC-1 AC-2 AC-5 AC-6 AU-1 AU-6 SI-1 SI-4

ArcGIS Online Cloud Controls Matrix (CCM) Answers

Control Area	Control ID	Control Specification	ArcGIS Online Response	Scope Applicability	
				ISO/IEC 27001-2005	NIST 800-53 R3
Information Security - User Responsibility	IS-16	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	ArcGIS Online employees adhere to a rules of behavior policy outlining user responsibilities.	Clause 5.2.2 A.8.2.2 A.11.3.1 A.11.3.2	AT-2 AT-3 AT-4 PL-4
Information Security - Workspace	IS-17	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 procedural controls are part of ArcGIS Online's policies including areas such as defined session time-out requirements.	Clause 5.2.2 A.8.2.2 A.9.1.5 A.11.3.1 A.11.3.2 A.11.3.3	AC-11 MP-2 MP-3 MP-4
Information Security - Encryption	IS-18	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).	ArcGIS Online provides customer's administrator the option of requiring encryption-in-transit via HTTPS (TLS) for customer data transmitted to and from their ArcGIS Online organization. ArcGIS Online does not encrypt customer data at rest. Customer can encrypt their data either through their application or by leveraging an enterprise cloud encryption gateway solution. Customers with data sensitivity concerns frequently choose to implement a hybrid solution where more sensitive data is kept on-premises or in a separate cloud with higher security reassurance, such as Esri Managed Cloud Services (http://doc.arcgis.com/en/trust/security/esri-managed-cloud-services.htm).	A.10.6.1 A.10.8.3 A.10.8.4 A.10.9.2 A.10.9.3 A.12.3.1 A.15.1.3 A.15.1.4	AC-18 IA-3 IA-7 SC-7 SC-8 SC-9 SC-13 SC-16 SC-23 SI-8
Information Security - Encryption Key Management	IS-19	Policies and procedures shall be established and mechanisms implemented for effective key management to support encryption of data in storage and in transmission.	ArcGIS Online operational keys are managed by the ArcGIS Online Operations Leads. Critical keys are rotated periodically during product release time windows. Compromised keys are revoked and reissued within 24 hours of detection.	Clause 4.3.3 A.10.7.3 A.12.3.2 A.15.1.6	SC-12 SC-13 SC-17 SC-28

ArcGIS Online Cloud Controls Matrix (CCM) Answers

Control Area	Control ID	Control Specification	ArcGIS Online Response	Scope Applicability	
				ISO/IEC 27001-2005	NIST 800-53 R3
Information Security - Vulnerability / Patch Management	IS-20	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 vendor-supplied security patches applied in a timely manner taking a risk-based approach for prioritizing critical patches.	ArcGIS Online releases which include patches and bug fixes are performed quarterly. If security vulnerabilities are found or reported, they are assessed by security staff. Any vulnerabilities that have an assessed risk of high or critical are patched immediately outside of normal patching routines.	A.12.5.1 A.12.5.2 A.12.6.1	CM-3 CM-4 CP-10 RA-5 SA-7 SI-1 SI-2 SI-5
Information Security - Anti-Virus / Malicious Software	IS-21	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.	A number of key security parameters are monitored to identify potentially malicious activity on the systems. Cloud infrastructure provider anti-virus controls align with ISO 27001 requirements.	A.10.4.1	SA-7 SC-5 SI-3 SI-5 SI-7 SI-8
Information Security - Incident Management	IS-22	Policies and procedures shall be established to triage security related events and ensure timely and thorough incident management.	Incident management is delineated within ArcGIS Online's Incident Response Plan documentation aligning with FISMA requirements.	Clause 4.3.3 A.13.1.1 A.13.2.1	IR-1 IR-2 IR-3 IR-4 IR-5 IR-7 IR-8
Information Security - Incident Reporting	IS-23	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.	ArcGIS Online's incident response program, plans and procedures have been developed in alignment with FISMA requirements. Esri notifies the customer of a confirmed breach that impacts the customer's data or information within 72 hours. Esri will coordinate with appropriate parties to investigate the security breach and take commercially reasonable steps for remediation based on Esri's assessment of risk. Esri will provide updates to the customer with applicable information on a mutually agreed upon schedule.	Clause 4.3.3 Clause 5.2.2 A.6.1.3 A.8.2.1 A.8.2.2 A.13.1.1 A.13.1.2 A.13.2.1	IR-2 IR-6 IR-7 SI-4 SI-5

ArcGIS Online Cloud Controls Matrix (CCM) Answers

Control Area	Control ID	Control Specification	ArcGIS Online Response	Scope Applicability	
				ISO/IEC 27001-2005	NIST 800-53 R3
Information Security - Incident Response Legal Preparation	IS-24	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.	ArcGIS Online's incident response program, plans and procedures have been developed in alignment with FISMA requirements.	Clause 4.3.3 Clause 5.2.2 A.8.2.2 A.8.2.3 A.13.2.3 A.15.1.3	AU-6 AU-7 AU-9 AU-11 IR-5 IR-7 IR-8
Information Security - Incident Response Metrics	IS-25	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.	A.13.2.2	IR-4 IR-5 IR-8
Information Security - Acceptable Use	IS-26	Policies and procedures shall be established for the acceptable use of information assets.	Prior to granting access to ArcGIS Online services, customers are required to review and agree to the terms of use. The ArcGIS Online terms of use are available at: http://www.esri.com/legal/pdfs/mla_e204_e300/english.html/#Addendum_3 The Esri Employee Handbook specifies acceptable terms of use for all employees. For employees that work with ArcGIS Online, a suplementary Rules of Behaviour (ROB) document is signed.	A.7.1.3	AC-8 AC-20 PL-4
Information Security - Asset Returns	IS-27	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 notified to destroy or return, as applicable, any physical materials that Esri 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.	A.7.1.1 A.7.1.2 A.8.3.2	PS-4
Information Security - eCommerce Transactions	IS-28	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.	ArcGIS Online does not provide e-commerce solutions.	A.7.2.1 A.10.6.1 A.10.6.2 A.10.9.1 A.10.9.2 A.15.1.4	AC-14 AC-21 AC-22 IA-8 AU-10 SC-4
Information Security - Audit Tools Access	IS-29	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 ArcGIS Online.	A.15.3.2	AU-9 AU-11 AU-14

ArcGIS Online Cloud Controls Matrix (CCM) Answers

Control Area	Control ID	Control Specification	ArcGIS Online Response	Scope Applicability	
				ISO/IEC 27001-2005	NIST 800-53 R3
Information Security - Diagnostic / Configuration Ports Access	IS-30	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	Access to information system diagnostic and configuration ports is restricted to authorized personnel within ArcGIS Online.	A.10.6.1 A.11.1.1 A.11.4.4 A.11.5.4	CM-7 MA-3 MA-4 MA-5
Information Security - Network / Infrastructure Services	IS-31	Network and infrastructure service level agreements (in-house or outsourced) shall clearly document security controls, capacity and service levels, and business or customer requirements.	Amazon Web Services and Microsoft Azure public service level agreements are available for review through the respective service providers. Azure's main underlying network infrastructure is currently managed by Microsoft's Global Foundation Services (GFS). SLAs to service providers or equipment manufacturers are qualified by GFS's ISO 27001 certification. Microsoft Azure SLA information is available at: http://www.windowsazure.com/en-us/support/legal/sla/ . Amazon Web Services EC2 SLA information is available at: http://aws.amazon.com/ec2-sla/ other AWS component SLA's are also available at this site.	A.6.2.3 A.10.6.2	SC-20 SC-21 SC-22 SC-23 SC-24
Information Security - Portable / Mobile Devices	IS-32	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).	Cloud infrastructure provider 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 cloud infrastructure management.	A.7.2.1 A.10.7.1 A.10.7.2 A.10.8.3 A.11.7.1 A.11.7.2 A.15.1.4	AC-17 AC-18 AC-19 MP-2 MP-4 MP-6
Information Security - Source Code Access Restriction	IS-33	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.	ArcGIS Online source code libraries are limited to authorized personnel. 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.	Clause 4.3.3 A.12.4.3 A.15.1.3	CM-5 CM-6
Information Security - Utility Programs Access	IS-34	Utility programs capable of potentially overriding system, object, network, virtual machine and application controls shall be restricted.	Access to information systems utility programs are restricted to authorized personnel within ArcGIS Online.	A.11.4.1 A 11.4.4 A.11.5.4	AC-5 AC-6 CM-7 SC-3 SC-19

ArcGIS Online Cloud Controls Matrix (CCM) Answers

Control Area	Control ID	Control Specification	ArcGIS Online Response	Scope Applicability	
				ISO/IEC 27001-2005	NIST 800-53 R3
Legal - Non-Disclosure Agreements	LG-01	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.	Esri Legal Counsel manages and periodically revises the Esri NDA to reflect ArcGIS Online business needs.	Annex A.6.1.5	PL-4 PS-6 SA-9
Legal - Third Party Agreements	LG-02	Third party agreements that directly, or indirectly, impact the organizations information assets or data are required to include explicit coverage of all relevant security requirements. This includes agreements involving processing, accessing, communicating, hosting or managing the organization's information assets, or adding or terminating services or products to existing information. Assets agreements provisions shall include security (e.g., encryption, access controls, and leakage prevention) and integrity controls for data exchanged to prevent improper disclosure, alteration or destruction.	Third party agreements are reviewed by Esri Contracts and/or Legal Counsel as appropriate.	A.6.2.3 A10.2.1 A.10.8.2 A.11.4.6 A.11.6.1 A.12.3.1 A.12.5.4	CA-3 MP-5 PS-7 SA-6 SA-7 SA-9
Operations Management - Policy	OP-01	Policies and procedures shall be established and made available for all personnel to adequately support services operations role.	Consistent with Esri policy, hiring managers define job requirements prior to recruiting, interviewing, and hiring. Job requirements include the primary responsibilities and tasks involved in the job, background characteristics needed to perform the job, and personal characteristics required. Once the requirements are determined, managers create a job description, which is a profile of the job and is used to identify potential candidates. When viable candidates are identified, the interview process begins to evaluate candidates and to make an appropriate hiring decision.	Clause 5.1 A 8.1.1 A.8.2.1 A 8.2.2 A.10.1.1	CM-2 CM-3 CM-4 CM-5 CM-6 CM-9 MA-4 SA-3 SA-4 SA-5 SA-8 SA-10 SA-11 SA-12
Operations Management - Documentation	OP-02	Information system documentation (e.g., administrator and user guides, architecture diagrams, etc.) shall be made available to authorized personnel to ensure the following: • Configuring, installing, and operating the information system • Effectively using the system's security features	Information System Documentation is made available internal to ArcGIS Online personnel through the use of Esri's Intranet site. For security and operational reasons, Esri does not provide internal operations documentation with customers.	Clause 4.3.3 A.10.7.4	CP-9 CP-10 SA-5 SA-10 SA-11

ArcGIS Online Cloud Controls Matrix (CCM) Answers

Control Area	Control ID	Control Specification	ArcGIS Online Response	Scope Applicability	
				ISO/IEC 27001-2005	NIST 800-53 R3
Operations Management - Capacity / Resource Planning	OP-03	The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with regulatory, contractual and business requirements. Projections of future capacity requirements shall be made to mitigate the risk of system overload.	ArcGIS Online utilizes the capacity of two major cloud infrastructure providers to meet customer demands. Each cloud provider offers SLAs for their infrastructure - Esri provides an SLA for ArcGIS Online available at: http://www.esri.com/~/media/Files/Pdfs/legal/pdfs/g-632-ArcGIS Online-service-level.pdf.	A.10.3.1	SA-4
Operations Management - Equipment Maintenance	OP-04	Policies and procedures shall be established for equipment maintenance ensuring continuity and availability of operations.	Cloud infrastructure providers ensure continuity of operations during equipment maintenance. If an upgrade of ArcGIS Online requires an outage window, customers will be notified ahead of time.	A.9.2.4	MA-2 MA-3 MA-4 MA-5 MA-6
Risk Management - Program	RI-01	Organizations shall develop and maintain an enterprise risk management framework to manage risk to an acceptable level.	ArcGIS Online provides customer remuneration for losses they may incur due to outages in alignment with ArcGIS Online Service Level Agreement available at: http://www.esri.com/~/media/Files/Pdfs/legal/pdfs/g-632-ArcGIS Online-service-level.pdf.	Clause 4.2.1 c) through g) Clause 4.2.2 b) Clause 5.1 f) Clause 7.2 & 7.3 A.6.2.1	AC-4 CA-2 CA-6 PM-9 RA-1
Risk Management - Assessments	RI-02	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk should be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).	Risk Assessments are performed on a regular basis and a continuous monitoring plan is in place as specified by FISMA requirements for ArcGIS Online.	Clause 4.2.1 c) through g) Clause 4.2.3 d) Clause 5.1 f) Clause 7.2 & 7.3 A.6.2.1 A.12.5.2 A.12.6.1 A.14.1.2 A.15.1.1 A.15.2.1 A.15.2.2	PL-5 RA-2 RA-3

ArcGIS Online Cloud Controls Matrix (CCM) Answers

Control Area	Control ID	Control Specification	ArcGIS Online Response	Scope Applicability	
				ISO/IEC 27001-2005	NIST 800-53 R3
Risk Management - Mitigation / Acceptance	RI-03	Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and executive approval.	The ArcGIS Online FISMA based Risk Assessment Assess phase begins with identifying risks, establishing a risk level by determining the likelihood of occurrence and impact, and finally, identifying controls and safeguards that reduce the impact of the risk to an acceptable level. Accordingly, measures, recommendations and controls are put in place to mitigate the risks to the extent possible.	Clause 4.2.1 c) through g) Clause 4.2.2 b) Clause 4.3.1 Clause 5.1 f) Clause 7.3 A.6.2.1 A.12.5.2 A.12.6.1 A.15.1.1 A.15.2.1 A.15.2.2	CA-5 CM-4
Risk Management - Business / Policy Change Impacts	RI-04	Risk assessment results shall include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective.	Decisions to update policies and procedures are based on the risk assessment reports. Risk Assessments are regularly reviewed based on periodicity and changes emerging to the risk landscape.	Clause 4.2.3 Clause 4.2.4 Clause 4.3.1 Clause 5 Clause 7	CP-2 RA-2 RA-3
Risk Management - Third Party Access	RI-05	The identification, assessment, and prioritization of risks posed by business processes requiring third party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.	Third party cloud infrastructure provider access to ArcGIS Online customer data is heavily restricted. Cloud infrastructure provider access is only available on a need-to-know basis and managed by their ISO 27001 security controls.	A.6.2.1 A.8.3.3 A.11.1.1 A.11.2.1 A.11.2.4	CA-3 MA-4 RA-3
Release Management - New Development / Acquisition	RM-01	Policies and procedures shall be established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities.	Esri maintains separate non-production systems for testing and validating new development and systems infrastructure capabilities as outlined in the internal ArcGIS Online Configuration Management Plan, aligning with FISMA requirements.	A.6.1.4 A.6.2.1 A.12.1.1 A.12.4.1 A.12.4.2 A.12.4.3	CA-1 CM-1 CM-9 PL-1 PL-2 SA-1

ArcGIS Online Cloud Controls Matrix (CCM) Answers

Control Area	Control ID	Control Specification	ArcGIS Online Response	Scope Applicability	
				ISO/IEC 27001-2005	NIST 800-53 R3
Release Management - Production Changes	RM-02	Changes to the production environment shall be documented, tested and approved prior to implementation. Production software and hardware changes may include applications, systems, databases and network devices requiring patches, service packs, and other updates and modifications.	For more information see RM-01.	A.10.1.4 A.12.5.1 A.12.5.2	CA-1 CA-6 CA-7 CM-2 CM-3 CM-5 CM-6 CM-9
Release Management - Quality Testing	RM-03	A program for the systematic monitoring and evaluation to ensure that standards of quality are being met shall be established for all software developed by the organization. Quality evaluation and acceptance criteria for information systems, upgrades, and new versions shall be established, documented and tests of the system(s) shall be carried out both during development and prior to acceptance to maintain security. Management shall have a clear oversight capacity in the quality testing process with the final product being certified as "fit for purpose" (the product should be suitable for the intended purpose) and "right first time" (mistakes should be eliminated) prior to release.	ArcGIS Online conducts testing and validation prior to release in accordance with FISMA Low requirements. Cloud infrastructure providers ensure changes are tested in various test environments and signed off prior to deployment into production and ensuring alignment with the ISO 27001 standard.	A.6.1.3 A.10.1.1 A.10.1.4 A.10.3.2 A.12.1.1 A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.4.1 A.12.4.2 A.12.4.3 A.12.5.1 A.12.5.2 A.12.5.3 A.12.6.1 A.13.1.2	CM-1 CM-2 SA-3 SA-4 SA-5 SA-8 SA-10 SA-11 SA-13

ArcGIS Online Cloud Controls Matrix (CCM) Answers

Control Area	Control ID	Control Specification	ArcGIS Online Response	Scope Applicability	
				ISO/IEC 27001-2005	NIST 800-53 R3
Release Management - Outsourced Development	RM-04	A program for the systematic monitoring and evaluation to ensure that standards of quality are being met shall be established for all outsourced software development. The development of all outsourced software shall be supervised and monitored by the organization and must include security requirements, independent security review of the outsourced environment by a certified individual, certified security training for outsourced software developers, and code reviews. Certification for the purposes of this control shall be defined as either a ISO/IEC 17024 accredited certification or a legally recognized license or certification in the legislative jurisdiction the organization outsourcing the development has chosen as its domicile.	Microsoft applies their Security Development Lifecycle, whereas Amazon typically does not outsource development of their software. Both providers solutions align with the ISO 27001 security standard.	A.6.1.8 A.6.2.1 A.6.2.3 A.10.1.4 A.10.2.1 A.10.2.2 A.10.2.3 A.10.3.2 A.12.1.1 A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.4.1 A.12.4.2 A.12.4.3 A.12.5.1 A.12.5.2	SA-4 SA-5 SA-8 SA-9 SA-10 SA-11 SA-12 SA-13
Release Management - Unauthorized Software Installations	RM-05	Policies and procedures shall be established and mechanisms implemented to restrict the installation of unauthorized software.	All production changes go through the Change Management process described in RM-01.	A.10.1.3 A.10.4.1 A.11.5.4 A.11.6.1 A.12.4.1	CM-1 CM-2 CM-3 CM-5 CM-7
Resiliency - Management Program	RS-01	Policy, process and procedures defining business continuity and disaster recovery shall be put in place to minimize the impact of a realized risk event on the organization to an acceptable level and facilitate recovery of information assets (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) through a combination of preventive and recovery controls, in accordance with regulatory, statutory, contractual, and business requirements and consistent with industry standards. This Resiliency management program shall be communicated to all organizational participants with a need to know basis prior to adoption and shall also be published, hosted, stored, recorded and disseminated to multiple facilities which must be accessible in the event of an incident.	The ArcGIS Online cloud infrastructure providers have business continuity policies and plans that are in alignment with ISO 27001 standards. ArcGIS Online has a contingency plan and utilizes redundant cloud infrastructure to minimize outages.	Clause 4.3.2 A.14.1.1 A 14.1.4	CP-1 CP-2

ArcGIS Online Cloud Controls Matrix (CCM) Answers

Control Area	Control ID	Control Specification	ArcGIS Online Response	Scope Applicability	
				ISO/IEC 27001-2005	NIST 800-53 R3
Resiliency - Impact Analysis	RS-02	There shall be a defined and documented method for determining the impact of any disruption to the organization which must incorporate the following: • Identify critical products and services • Identify all dependencies, including processes, applications, business partners and third party service providers • Understand threats to critical products and services • Determine impacts resulting from planned or unplanned disruptions and how these vary over time • Establish the maximum tolerable period for disruption • Establish priorities for recovery • Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption • Estimate the resources required for resumption	ArcGIS Online cloud infrastructure providers perform business impact analysis meeting ISO 27001 standards requirements. Customers may view infrastructure and application status information on the following dashboards: AWS: http://status.aws.amazon.com MS Azure: http://www.windowsazure.com/en-us/support/service-dashboard/ ArcGIS Online: http://status.arcgis.com	A.14.1.2 A 14.1.4	RA-3
Resiliency - Business Continuity Planning	RS-03	A consistent unified framework for business continuity planning and plan development shall be established, documented and adopted to ensure all business continuity plans are consistent in addressing priorities for testing and maintenance and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update and approval • Defined lines of communication, roles and responsibilities • Detailed recovery procedures, manual work-around and reference information • Method for plan invocation	Cloud infrastructure providers ensure their business continuity plans align with ISO 27001 standards.	Clause 5.1 A.6.1.2 A.14.1.3 A.14.1.4	CP-1 CP-2 CP-3 CP-4 CP-6 CP-7 CP-8 CP-9 CP-10 PE-17

ArcGIS Online Cloud Controls Matrix (CCM) Answers

Control Area	Control ID	Control Specification	ArcGIS Online Response	Scope Applicability	
				ISO/IEC 27001-2005	NIST 800-53 R3
Resiliency - Business Continuity Testing	RS-04	Business continuity plans shall be subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness.	Cloud infrastructure provider recovery plans are validated on a regular basis per industry best practices to ensure that solutions are viable at time of event.	A.14.1.5	CP-2 CP-3 CP-4
Resiliency - Environmental Risks	RS-05	Physical protection against damage from natural causes and disasters as well as deliberate attacks including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear mishap, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed and countermeasures applied.	Cloud infrastructure provider environmental controls have been implemented to protect the data center (aligning with ISO 27002 best practices) including: • Temperature control • Heating, Ventilation and Air Conditioning (HVAC) • Fire detection and suppression systems • Power Management systems	A.9.1.4 A.9.2.1	PE-1 PE-13 PE-14 PE-15 PE-18
Resiliency - Equipment Location	RS-06	To reduce the risks from environmental threats, hazards and opportunities for unauthorized access equipment shall be located away from locations subject to high probability environmental risks and supplemented by redundant equipment located a reasonable distance.	Windows Azure services equipment is placed in environments which have been engineered to be protective from theft and environmental risks such as fire, smoke, water, dust, vibration, earthquake, and electrical interference. AWS data centers incorporate physical protection against environmental risks. ArcGIS Online is architected to take advantage of utilizing services and data across multiple AWS Availability zones.	A.9.2.1	PE-1 PE-5 PE-14 PE-15 PE-18
Resiliency - Equipment Power Failures	RS-07	Security mechanisms and redundancies shall be implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.).	The data centers have dedicated 24x7 uninterruptible power supply (UPS) and emergency power support, which may include generators. Regular maintenance and testing is conducted for both the UPS and generators. Data centers have made arrangements for emergency fuel delivery.	A.9.2.2 A.9.2.3 A 9.2.4	CP-8 PE-1 PE-9 PE-10 PE-11 PE-12 PE-13 PE-14
Resiliency - Power / Telecommunications	RS-08	Telecommunications equipment, cabling and relays transceving data or supporting services shall be protected from interception or damage and designed with redundancies, alternative power source and alternative routing.	Cabling security and supporting utilities deployment with the cloud infrastructure providers meets the ISO 27001 standards, specifically addressed in Annex A, domains 9.2.3 and 9.2.2.	A.9.2.2 A.9.2.3	PE-1 PE-4 PE-13

ArcGIS Online Cloud Controls Matrix (CCM) Answers

Control Area	Control ID	Control Specification	ArcGIS Online Response	Scope Applicability	
				ISO/IEC 27001-2005	NIST 800-53 R3
Security Architecture - Customer Access Requirements	SA-01	Prior to granting customers access to data, assets and information systems, all identified security, contractual and regulatory requirements for customer access shall be addressed and remediated.	Prior to granting access to ArcGIS Online services, customers are required to review and agree to the terms of use. The ArcGIS Online terms of use are available at: http://www.esri.com/legal/pdfs/mla_e204_e300/english.html	A.6.2.1 A.6.2.2 A.11.1.1	CA-1 CA-2 CA-5 CA-6
Security Architecture - User ID Credentials	SA-02	Implement and enforce (through automation) user credential and password controls for applications, databases and server and network infrastructure, requiring the following minimum standards: • User identity verification prior to password resets. • If password reset initiated by personnel other than user (i.e., administrator), password must be immediately changed by user upon first use. • Timely access revocation for terminated users. • Remove/disable inactive user accounts at least every 90 days. • Unique user IDs and disallow group, shared, or generic accounts and passwords. • Password expiration at least every 90 days. • Minimum password length of at least seven (7) characters. • Strong passwords containing both numeric and alphabetic characters. • Allow password re-use after the last four (4) passwords used. • User ID lockout after not more than six (6) attempts. • User ID lockout duration to a minimum of 30 minutes or until administrator enables the user ID. • Re-enter password to reactivate terminal after session idle time for more than 15 minutes. • Maintain user activity logs for privileged access or access to sensitive data.	Organizations should utilize ArcGIS Online Enterprise Logins to meet all of their organizations username and password management requirements and for adherence to FISMA and ISO 27001 security requirements. Further information concerning ArcGIS Online Enterprise Logins may be found at: http://resources.arcgis.com/en/help/arcgisonline/010q/010q000000vs000000.htm If an Identity Provider (IdP) is not available. ArcGIS Online allows Administrators to implement a custom password policy for their ArcGIS Online organization. Other than User ID lockouts (which utilizes fixed settings) password policies can be customized to meet the SA-02 requirements and customer specific policy requirements. For more info on setting a custom password policy, see: https://doc.arcgis.com/en/arcgis-online/administer/configure-security.htm	A.8.3.3 A.11.1.1 A.11.2.1 A.11.2.3 A.11.2.4 A.11.5.5	AC-1 AC-2 AC-3 AC-11 AU-2 AU-11 IA-1 IA-2 IA-5 IA-6 IA-8 SC-10

ArcGIS Online Cloud Controls Matrix (CCM) Answers

Control Area	Control ID	Control Specification	ArcGIS Online Response	Scope Applicability	
				ISO/IEC 27001-2005	NIST 800-53 R3
Security Architecture - Data Security / Integrity	SA-03	Policies and procedures shall be established and mechanisms implemented to ensure security (e.g., encryption, access controls, and leakage prevention) and integrity of data exchanged between one or more system interfaces, jurisdictions, or with a third party shared services provider to prevent improper disclosure, alteration or destruction complying with legislative, regulatory, and contractual requirements.	Interconnection Service Agreements (ISA) are established between backend external systems and ArcGIS Online specifying security integrity requirements.	A.10.8.1 A.10.8.2 A.11.1.1 A.11.6.1 A.11.4.6 A.12.3.1 A.12.5.4 A.15.1.4	AC-1 AC-4 SC-1 SC-16
Security Architecture - Application Security	SA-04	Applications shall be designed in accordance with industry accepted security standards (i.e., OWASP for web applications) and complies with applicable regulatory and business requirements.	As part of the FISMA accreditation requirements, ArcGIS Online is scanned on a regular basis for alignment with industry accepted security standards such as OWASP.	A.11.5.6 A.11.6.1 A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.5.2 A.12.5.4 A.12.5.5 A.12.6.1 A.15.2.1	SC-2 SC-3 SC-4 SC-5 SC-6 SC-7 SC-8 SC-9 SC-10 SC-11 SC-12
Security Architecture - Data Integrity	SA-05	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data.	ArcGIS Online utilizes relational databases to manage the integrity of feature datasets uploaded by customers. The cloud infrastructure providers ensure data integrity is maintained through all phases including transmission, storage, and processing.	A.10.9.2 A.10.9.3 A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.6.1 A.15.2.1	SI-10 SI-11 SI-2 SI-3 SI-4 SI-6 SI-7 SI-9
Security Architecture - Production / Non-Production Environments	SA-06	Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets.	ArcGIS Online utilizes separate production and non-production environments.	A.10.1.4 A.10.3.2 A.11.1.1 A.12.5.1 A.12.5.2 A.12.5.3	SC-2

ArcGIS Online Cloud Controls Matrix (CCM) Answers

Control Area	Control ID	Control Specification	ArcGIS Online Response	Scope Applicability	
				ISO/IEC 27001-2005	NIST 800-53 R3
Security Architecture - Remote User Multi-Factor Authentication	SA-07	Multi-factor authentication is required for all remote user access.	ArcGIS Online users can configure their Enterprise Logins to utilize their organization's two factor authentication solution which can align with requirements such as: HSPD-12, PIV, and CAC. In addition, customers can choose to enable multi-factor authentication for their ArcGIS Organization independent of Enterprise Logins. For more information, see: https://doc.arcgis.com/en/arcgis-online/reference/multifactor.htm Cloud infrastructure providers ensure two-factor authentication is utilized for their administrative operations.	A.11.1.1 A.11.4.1 A.11.4.2 A.11.4.6 A.11.7.1	AC-17 AC-20 IA-1 IA-2 MA-4
Security Architecture - Network Security	SA-08	Network environments shall be designed and configured to restrict connections between trusted and untrusted networks and reviewed at planned intervals, documenting the business justification for use of all services, protocols, and ports allowed, including rationale or compensating controls implemented for those protocols considered to be insecure. Network architecture diagrams must clearly identify high-risk environments and data flows that may have regulatory compliance impacts.	The cloud infrastructure providers utilize multiple separate network segments. This infrastructure provider segmentation helps to provide separation of critical, back-end servers and storage devices from the public-facing interfaces.	A.10.6.1 A.10.6.2 A.10.9.1 A.10.10.2 A.11.4.1 A.11.4.5 A.11.4.6 A.11.4.7 A.15.1.4	SC-7
Security Architecture - Segmentation	SA-09	System and network environments are separated by firewalls to ensure the following requirements are adhered to: • Business and customer requirements • Security requirements • Compliance with legislative, regulatory, and contractual requirements • Separation of production and non-production environments • Preserve protection and isolation of sensitive data	Cloud infrastructure provider network segmentation aligns with ISO 27001 standards. Cloud infrastructure provider firewalls and host based firewalls are utilized to separate various ArcGIS Online components.	A.11.4.5 A.11.6.1 A.11.6.2 A.15.1.4	AC-4 SC-2 SC-3 SC-7

ArcGIS Online Cloud Controls Matrix (CCM) Answers

Control Area	Control ID	Control Specification	ArcGIS Online Response	Scope Applicability	
				ISO/IEC 27001-2005	NIST 800-53 R3
Security Architecture - Wireless Security	SA-10	Policies and procedures shall be established and mechanisms implemented to protect wireless network environments, including the following: • Perimeter firewalls implemented and configured to restrict unauthorized traffic • Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, SNMP community strings, etc.). • Logical and physical user access to wireless network devices restricted to authorized personnel • The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network	Protection of wireless devices and ensuring encryption are part of regular network management security practices within Esri (includes monitoring). Access from a wireless network on a customer premise to the ArcGIS Online environment must be secured by the customer.	A.7.1.1 A.7.1.2 A.7.1.3 A.9.2.1 A.9.2.4 A.10.6.1 A.10.6.2 A.10.8.1 A.10.8.3 A.10.8.5 A.10.10.2 A.11.2.1 A.11.4.3 A.11.4.5 A.11.4.6 A.11.4.7 A.12.3.1 A.12.3.2	AC-1 AC-18 CM-6 PE-4 SC-3 SC-7
Security Architecture - Shared Networks	SA-11	Access to systems with shared network infrastructure shall be restricted to authorized personnel in accordance with security policies, procedures and standards. Networks shared with external entities shall have a documented plan detailing the compensating controls used to separate network traffic between organizations.	Cloud infrastructure shared network access is strictly restricted to critical resources including services, hosts, and network devices and must be explicitly approved.	A.10.8.1 A.11.1.1 A.11.6.2 A.11.4.6	PE-4 SC-4 SC-7
Security Architecture - Clock Synchronization	SA-12	An external accurate, externally agreed upon, time source shall be used to synchronize the system clocks of all relevant information processing systems within the organization or explicitly defined security domain to facilitate tracing and reconstitution of activity timelines. Note: specific legal jurisdictions and orbital storage and relay platforms (US GPS & EU Galileo Satellite Network) may mandate a reference clock that differs in synchronization with the organizations domicile time reference, in this event the jurisdiction or platform is treated as an explicitly defined security domain.	In order to increase the security of ArcGIS Online all services use consistent clock setting standards (e.g. PST, GMT, UTC etc.). When possible, server clocks are synchronized through the Network Time Protocol which hosts a central time source for standardization and reference, in order to maintain accurate time throughout ArcGIS Online systems.	A.10.10.1 A.10.10.6	AU-1 AU-8

ArcGIS Online Cloud Controls Matrix (CCM) Answers

Control Area	Control ID	Control Specification	ArcGIS Online Response	Scope Applicability	
				ISO/IEC 27001-2005	NIST 800-53 R3
Security Architecture - Equipment Identification	SA-13	Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.	Cloud infrastructure providers manage equipment identification in alignment with the ISO 27001 standard.	A.11.4.3	IA-3 IA-4
Security Architecture - Audit Logging / Intrusion Detection	SA-14	Audit logs recording privileged user access activities, authorized and unauthorized access attempts, system exceptions, and information security events shall be retained, complying with applicable policies and regulations. Audit logs shall be reviewed at least daily and file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents. Physical and logical user access to audit logs shall be restricted to authorized personnel.	Access to logs is restricted as defined by policy, and logs are reviewed on a regular basis as required by FISMA.	A.10.10.1 A.10.10.2 A.10.10.3 A.10.10.4 A.10.10.5 A.11.2.2 A.11.5.4 A.11.6.1 A.13.1.1 A.13.2.3 A.15.2.2 A.15.1.3	AU-1 AU-2 AU-3 AU-4 AU-5 AU-6 AU-7 AU-9 AU-11 AU-12 AU-14 SI-4
Security Architecture - Mobile Code	SA-15	Mobile code shall be authorized before its installation and use, and the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy. All unauthorized mobile code shall be prevented from executing.	ArcGIS Online does not require installable mobile code such as MS ActiveX, Adobe Flash, and MS Silverlight	A.10.4.2 A.12.2.2	SC-18