ArcGIS Online
Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) 3.0.1
August 2018

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 133 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 the CSA CCM since 2013, and will update this document focused on ArcGIS Online for newer CCM revisions in the future.

Significant changes to version 3.x CCM from the previous version 1.x CCM include:

- Five new control domains that address information security risks over the access of, transfer to, and securing of cloud data: Mobile Security; Supply Chain Management, Transparency & Accountability; Interoperability & Portability; and Encryption & Key Management
- Improved harmonization with the Security Guidance for Critical Areas of Cloud Computing v3
- Improved control auditability throughout the control domains and an expanded control identification naming convention
- Incremental updates/corrections of version 3.0.1 questions are made available by the CSA. We've incorporated updates for version 3.0.1 10/6/2016 within this document.

ArcGIS Online was granted a Federal Risk and Authorization Management Program (FedRAMP) Tailored Low Authority to Operate (ATO) by the United States Department of Interior. For more information concerning the security, privacy and compliance of ArcGIS Online please see the Trust Center at: 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's Software Security & Privacy Team at:
SoftwareSecurity@Esri.com

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	Supplier Relationship		Scope Applicability	
				Service Provider	Tenant / Consumer	ISO/IEC 27001:2013	FedRAMP --LOW IMPACT--
Application & Interface Security Application Security	AIS-01	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Building and validating ArcGIS Online code against leading security industry standards such as OWASP is the foundation for building a robust offering. This is enforced within the continuous monitoring requirements of the ArcGIS Online FedRAMP authorization. ArcGIS Online is scanned at a minimum of every 30 days to ensure services are regularly validated against standards such as OWASP.	X		A9.4.2 A9.4.1, 8.1*Partial, A14.2.3, 8.1*partial, A.14.2.7 A12.6.1, A18.2.2	NIST SP 800-53 R3 SC-5 NIST SP 800-53 R3 SC-6 NIST SP 800-53 R3 SC-7 NIST SP 800-53 R3 SC-12 NIST SP 800-53 R3 SC-13 NIST SP 800-53 R3 SC-14
Application & Interface Security Customer Access Requirements	AIS-02	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	Before using ArcGIS Online, customers are required to review and agree with the acceptable use of data and ArcGIS Online service, as well as security and privacy requirements, which are defined in the Terms of Service @ http://www.esri.com/legal/pdfs/mla_e204_e300/english#Addendum_3 and Privacy policy @ http://www.esri.com/legal/privacy-arcgis. ArcGIS Online maintains a FedRAMP Tailored Low security authorization through the US Government and utilizes cloud infrastructure providers that are ISO 27001 compliant. It is also Privacy Shield compliant and aliigns with GDPR for privacy assurance. Additional information concerning the security and privacy of ArcGIS Online may be found within the Trust.ArcGIS.com website.	X	X	A9.1.1.	NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 CA-5 NIST SP 800-53 R3 CA-6
Application & Interface Security Data Integrity	AIS-03	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	Customers can choose to require HTTPS (TLS) for their ArcGIS Online organization to ensure integrity of data in transit. ArcGIS Online utilizes relational databases to manage the integrity of feature datasets uploaded by customers. The cloud infrastructure providers are compliant with ISO 27001 and ensure data integrity is maintained through all phases including transmission, storage and processing.	X	X	A13.2.1, A13.2.2, A9.1.1, A9.4.1, A10.1.1 A18.1.4	NIST SP 800-53 R3 SI-2 NIST SP 800-53 R3 SI-3
Application & Interface Security Data Security / Integrity	AIS-04	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction.	Esri's Corporate Security policies are based on NIST 800-53 security controls which map to ISO 27001 controls. ArcGIS Online data security measures are in alignment with FedRAMP Tailored Low requirements (that have NIST 800-53 security controls as it's core). ArcGIS Online procedures include requiring that updates are reviewed for unauthorized changes during the release management process. ArcGIS Online's cloud infrastructure providers data security policies, procedures, and processes align with industry standards such as FedRAMP Moderate and ISO 27001.	X		A13.2.1, A13.2.2, A9.1.1, A9.4.1, A10.1.1 A18.1.4	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SC-13

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	Supplier Relationship		Scope Applicability	
				Service Provider	Tenant / Consumer	ISO/IEC 27001:2013	FedRAMP --LOW IMPACT--
Audit Assurance & Compliance Audit Planning	AAC-01	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.	Esri employs a fulltime information assurance team to ensure audits are appropriately planned and coordinated. ArcGIS Online is audited in accordance with FedRAMP Tailored Low requirements which includes ensuring auditors provide an audit plan and agree to Rules of Engagement terms before executing an audit. ArcGIS Online utilizes cloud infrastructure from Microsoft Azure, and Amazon Web Services. Each of the cloud infrastructure providers regularly audit their operations and can provide them under their own NDA's.	X		Clauses 4.3(a), 4.3(b), 5.1(e), 5.1(f), 6.2(e), 9.1, 9.1(e), 9.2, 9.3(f), A12.7.1	NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 CA-7
Audit Assurance & Compliance Independent Audits	AAC-02	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.	Independent audits of security controls in place for ArcGIS Online are conducted at least annually in alignment with FedRAMP Tailored Low requirements. Cloud infrastructure providers are subjected to regular internal and external audits (at least annually) in alignment with FedRAMP Moderate and ISO 27001 requirements.	X	X	Clauses 4.3(a), 4.3(b), 5.1(e), 5.1(f), 9.1, 9.2, 9.3(f), A18.2.1	NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 CA-6 NIST SP 800-53 R3 RA-5
Audit Assurance & Compliance Information System Regulatory Mapping	AAC-03	Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.	FedRAMP authorization is based on the NIST 800-53 control framework helping ensure ArcGIS Online complies with applicable data protection and privacy laws. ArcGIS Online has an established process for identifying and implementing changes to services in response to changes in applicable statutes and regulations. 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 monitor and update all relevant and regulatory requirements with processes that align with FedRAMP Moderate and ISO 27001.	X	X	Clauses 4.2(b), 4.4, 5.2(c), 5.3(ab), 6.1.2, 6.1.3, 6.1.3(b), 7.5.3(b), 7.5.3(d), 8.1, 8.3 9.2(g), 9.3, 9.3(b), 9.3(f), 10.2, A.8.2.1, A.18.1.1, A.18.1.3, A.18.1.4, A.18.1.5	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IA-7 NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	Supplier Relationship		Scope Applicability	
				Service Provider	Tenant / Consumer	ISO/IEC 27001:2013	FedRAMP --LOW IMPACT--
Business Continuity Management & Operational Resilience Business Continuity Planning	BCR-01	A consistent unified framework for business continuity planning and plan development shall be established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update, and approval • Defined lines of communication, roles, and responsibilities • Detailed recovery procedures, manual work-around, and reference information • Method for plan invocation	ArcGIS Online has a full Continuity Plan designed in alignment with FedRAMP securiy control requirements. ArcGIS Online cloud Infrastructure providers ensure their business continuity plans align with ISO 27001 standards.	X	X	Clause 5.1(h) A.17.1.2 A.17.1.2	NIST SP800-53 R3 CP-1 NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-3 NIST SP800-53 R3 CP-4 NIST SP800-53 R3 CP-9 NIST SP800-53 R3 CP-10
Business Continuity Management & Operational Resilience Business Continuity Testing	BCR-02	Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.	ArcGIS Online does contingency plan and incident response plan testing at a minimum of annually in alignment with FedRAMP Tailored Low requirements. ArcGIS Online's cloud infrastructure providers business continuity policies, plans, and processes are developed and tested in alignment with ISO 27001 standards.	X	X	A17.3.1	NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-3 NIST SP800-53 R3 CP-4
Business Continuity Management & Operational Resilience Datacenter Utilities / Environmental Conditions	BCR-03	Data center utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.	ArcGIS Online uses cloud infrastructure providers whose datacenters comply with industry standards (such as ISO 27001) for physical security and availability.	X		A11.2.2, A11.2.3	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-13 (1) NIST SP800-53 R3 PE-13 (2) NIST SP800-53 R3 PE-13 (3)
Business Continuity Management & Operational Resilience Documentation	BCR-04	Information system documentation (e.g., administrator and user guides, and architecture diagrams) 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 to customers. For best practice security implementation guidance for customer organizations in ArcGIS Online, see: https://doc.arcgis.com/en/trust/security/arcgis-online-best-practices.htm. There are also detailed user guides available in the online help section for ArcGIS Online: http://doc.arcgis.com/en/arcgis-online/	X		Clause 9.2(g) A12.1.1	NIST SP 800-53 R3 CP-9 NIST SP 800-53 R3 CP-10 NIST SP 800-53 R3 SA-5
Business Continuity Management & Operational Resilience Environmental Risks	BCR-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 accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.	Cloud infrastructure provider environmental controls have been implemented to protect the data center (complying with ISO 27001) including: -Temperature control -Heating, Ventilation and Air Conditioning (HVAC) -Fire detection and suppression systems -Power Management systems	X		A11.1.4, A11.2.1 A11.2.2	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-14 NIST SP800-53 R3 PE-15

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	Supplier Relationship		Scope Applicability	
				Service Provider	Tenant / Consumer	ISO/IEC 27001:2013	FedRAMP --LOW IMPACT--
Business Continuity Management & Operational Resilience Equipment Location	BCR-06	To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.	Windows Azure services' equipment is place in environments which have been engineered to be protected from theft and environmental risks such as fire, smoke, water, dust, vibration, earthquakes, and electrical interference. AWS data centers incorporate physical protection against environmental risks. AWS services provide customers the flexibility to store data within multiple geographical regions as well as across multiple Availability Zones. Customers should architect their AWS usage to take advantage of multiple Regions and Availability Zones.	X		A11.2.1	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-14 NIST SP800-53 R3 PE-15
Business Continuity Management & Operational Resilience Equipment Maintenance	BCR-07	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.	Cloud infrastructure providers ensure continuity of operations during equipment maintenance. If an upgrade of ArcGIS Online require an outage window, customers will be notified ahead of time.	X		A11.2.4	NIST SP 800-53 R3 MA-2 NIST SP 800-53 R3 MA-4 NIST SP 800-53 R3 MA-5
Business Continuity Management & Operational Resilience Equipment Power Failures	BCR-08	Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific business impact assessment.	The cloud infrastructure providers' data centers have 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.	X		A.11.2.2, A.11.2.3, A.11.2.4	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-12 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-14
Business Continuity Management & Operational Resilience Impact Analysis	BCR-09	There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following: • Identify critical products and services • Identify all dependencies, including processes, applications, business partners, and third party service providers • Understand threats to critical products and services • Determine impacts resulting from planned or unplanned disruptions and how these vary over time • Establish the maximum tolerable period for disruption • Establish priorities for recovery • Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption • Estimate the resources required for resumption	ArcGIS Online cloud infrastructure providers perform business impact analysis (BIA) 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	X	X	A.17.1.1 A.17.1.2	NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 CP-2 NIST SP 800-53 R3 RA-3

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	Supplier Relationship		Scope Applicability	
				Service Provider	Tenant / Consumer	ISO/IEC 27001:2013	FedRAMP --LOW IMPACT--
Business Continuity Management & Operational Resilience Policy	BCR-10	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery, and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular workforce training.	ArcGIS Online's cloud infrastructure providers have developed Business Continuity documentation that align with ISO 27001 and FedRAMP Moderate Requirements.	X		Clause 5.1(h) A.6.1.1 A.7.2.1 A.7.2.2 A.12.1.1	NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 CM-4 NIST SP 800-53 R3 CM-6 NIST SP 800-53 R3 MA-4 NIST SP 800-53 R3 SA-3 NIST SP 800-53 R3 SA-4 NIST SP 800-53 R3 SA-5
Business Continuity Management & Operational Resilience Retention Policy	BCR-11	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.	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: https://support.esri.com/en/technical-article/000011795	X	X	Clauses 9.2(g) 7.5.3(b) 5.2 (c) 7.5.3(d) 5.3(a) 5.3(b) 8.1 8.3 A.12.3.1 A.8.2.3	NIST SP 800-53 R3 CP-2 NIST SP 800-53 R3 CP-9
Change Control & Configuration Management New Development / Acquisition	CCC-01	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network, and systems components, or any corporate, operations and/or data center facilities have been pre-authorized by the organization's business leadership or other accountable business role or function.	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 FedRAMP Tailored Low requirements.	X		A.14.1.1 A.12.5.1 A.14.3.1 A.9.4.5 8.1* (partial) A.14.2.7 A.18.1.3 A.18.1.4	NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 PL-2 NIST SP 800-53 R3 SA-1 NIST SP 800-53 R3 SA-3 NIST SP 800-53 R3 SA-4
Change Control & Configuration Management Outsourced Development	CCC-02	External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g., ITIL service management processes).	Microsoft 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.	X	X	A18.2.1 A.15.1.2 A.12.1.4 8.1* (partial) 8.1* (partial) A.15.2.1 8.1* (partial) A.15.2.2	NIST SP 800-53 R3 SA-4 NIST SP 800-53 R3 SA-5 NIST SP 800-53 R3 SA-9

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	Supplier Relationship		Scope Applicability	
				Service Provider	Tenant / Consumer	ISO/IEC 27001:2013	FedRAMP --LOW IMPACT--
Change Control & Configuration Management Quality Testing	CCC-03	Organizations shall follow a defined quality change control and testing process (e.g., ITIL Service Management) with established baselines, testing, and release standards that focus on system availability, confidentiality, and integrity of systems and services.	ArcGIS Online conducts testing and validation prior to release in alignment with FedRAMP Tailored 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.	X		A.6.1.1 A.12.1.1 A.12.1.4 A.14.2.9 A.14.1.1 A.12.5.1 A.14.3.1 A.9.4.5 8.1* partial A.14.2.2 8.1* partial	NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 SA-3 NIST SP 800-53 R3 SA-4 NIST SP 800-53 R3 SA-5
Change Control & Configuration Management Unauthorized Software Installations	CCC-04	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	All changes into production go through the Change Management process described in CCC-05.	X		A.6.1.2 A.12.2.1 A.9.4.4 A.9.4.1 A.12.5.1 8.1* (partial) A.14.2.4	NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 CM-7 NIST SP 800-53 R3 CM-8 NIST SP 800-53 R3 SA-6 NIST SP 800-53 R3 SA-7 NIST SP 800-53 R3 SI-1 NIST SP 800-53 R3 SI-3
Change Control & Configuration Management Production Changes	CCC-05	Policies and procedures shall be established for managing the risks associated with applying changes to: • Business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations. • Infrastructure network and systems components. Technical measures shall be implemented to provide assurance that all changes directly correspond to a registered change request, business-critical or customer (tenant), and/or authorization by, the customer (tenant) as per agreement (SLA) prior to deployment.	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 FedRAMP Tailored Low requirements.	X	X	A.12.1.4 8.1* (partial) A.14.2.2 8.1* (partial) A.14.2.3	NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-6 NIST SP 800-53 R3 CA-7 NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 CM-6 NIST SP 800-53 R3 PL-2 NIST SP 800-53 R3 PL-5 NIST SP 800-53 R3 SI-2

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	Supplier Relationship		Scope Applicability	
				Service Provider	Tenant / Consumer	ISO/IEC 27001:2013	FedRAMP --LOW IMPACT--
Data Security & Information Lifecycle Management Classification	DSI-01	Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.	Esri classifies datasets they own according to the Esri Technology Control Plan and then implements a standard set of Security and Privacy attributes. Esri treats all Customer Data in accordance with the commitment outlined in DSI-02. Datasets uploaded to ArcGIS Online are owned by the customer and they are responsible for classifying their dataset and handling accordingly. It is Customer's sole responsibility to ensure that Customer Content is suitable for use with Online Services. Examples of datasets not recommended for Online Services include: International Traffic in Arms Regulations (ITAR), Unclassified Controlled Technical Information (UCTI), and Protected Health Information (PHI).	X	X	A.8.2.1	NIST SP 800-53 R3 RA-2
Data Security & Information Lifecycle Management Data Inventory / Flows	DSI-02	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's geographically distributed (physical and virtual) applications and infrastructure network and systems components and/or shared with other third parties to ascertain any regulatory, statutory, or supply chain agreement (SLA) compliance impact, and to address any other business risks associated with the data. Upon request, provider shall inform customer (tenant) of compliance impact and risk, especially if customer data is used as part of the services.	ArcGIS Online is a FedRAMP Tailored Low authorized solution by the United States Department of Agriculture (USDA). This includes the requirement to adhere to robust continuous monitoring requirements and security controls are reviewed at a minimum of every three (3) years. As for cloud providers of Amazon Web Services and Microsoft Azure, they will not move ArcGIS Online data from Esri's chosen physical regions (All reside on U.S. soil).	X	X	Clause 4.2 5.2, 7.5, 8.1	
Data Security & Information Lifecycle Management Ecommerce Transactions	DSI-03	Data related to electronic commerce (ecommerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data.	Esri stores no payment instrument number information (e.g. credit card) within their systems for Products & Services. Esri utilizes a third party provider which has been audited by a Payment Card Industry Standard certified auditor to ensure your information remains secure. Payment information is transmitted directly to the provider via HTTPS for secure transmission so that payment data is never transmitted or stored by Esri Products & Services.	X	X	A.8.2.1 A.13.1.1 A.13.1.2 A.14.1.2 A.14.1.3 A.18.1.4	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 AC-22 NIST SP 800-53 R3 AU-1
Data Security & Information Lifecycle Management Handling / Labeling / Security Policy	DSI-04	Policies and procedures shall be established for the labeling, handling, and security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.	ArcGIS Online customers retain ownership of their data and may implement a labeling and handling policy and procedures to meet their requirements.	X	X	A.8.2.2 A.8.3.1 A.8.2.3 A.13.2.1	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PE-16 NIST SP 800-53 R3 SI-1 NIST SP 800-53 R3 SI-12

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	Supplier Relationship		Scope Applicability	
				Service Provider	Tenant / Consumer	ISO/IEC 27001:2013	FedRAMP --LOW IMPACT--
Data Security & Information Lifecycle Management Non-Production Data	DSI-05	Production data shall not be replicated or used in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.	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.	X		A.8.1.3 A.12.1.4 A.14.3.1 8.1* (partial) A.14.2.2.	
Data Security & Information Lifecycle Management Ownership / Stewardship	DSI-06	All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.	Data stored within ArcGIS Online meets FedRAMP Tailored Low categorized requirements. Customers are responsible for implementing workflows to enforce this categorization level. Customers retain full ownership of their data.	X		A.6.1.1 A.8.1.2 A.18.1.4	NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 PS-2 NIST SP 800-53 R3 RA-2 NIST SP 800-53 R3 SA-2
Data Security & Information Lifecycle Management Secure Disposal	DSI-07	Policies and procedures shall be established with supporting business processes and technical measures 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 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.	X		A.11.2.7 A.8.3.2	NIST SP 800-53 R3 MP-6 NIST SP 800-53 R3 PE-1
Datacenter Security Asset Management	DCS-01	Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership by defined roles and responsibilities.	ArcGIS Online cloud infrastructure providers have established policies and procedures for addressing their assets aligning with ISO 27001 standards.	X		Annex A.8	
Datacenter Security Controlled Access Points	DCS-02	Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.	ArcGIS Online's cloud infrastructure providers have physical security measures for their data centers that comply with high industry standards for physical security controls. For more information, visit their respective compliance sites below. Microsoft Azure: https://www.microsoft.com/en-us/trustcenter/Compliance Amazon Web Services: https://aws.amazon.com/compliance/	X		A.11.1.1 A.11.1.2	NIST SP 800-53 R3 PE-2 NIST SP 800-53 R3 PE-3 NIST SP 800-53 R3 PE-6 NIST SP 800-53 R3 PE-7 NIST SP 800-53 R3 PE-8

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	Supplier Relationship		Scope Applicability	
				Service Provider	Tenant / Consumer	ISO/IEC 27001:2013	FedRAMP --LOW IMPACT--
Datacenter Security Equipment Identification	DCS-03	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 maintain a current, documented and audited inventory of equipment and network components for which it is responsible. The cloud infrastructure providers managed automated mechanisms to detect discrepancies in device configuration by comparing them against the defined policies. Cloud infrastructure providers manage equipment identification in alignment with the ISO 27001 standard.	X			NIST SP 800-53 R3 IA-4
Datacenter Security Off-Site Authorization	DCS-04	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.	X		A.11.2.6 A.11.2.7	NIST SP 800-53 R3 AC-17 NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PE-16
Datacenter Security Off-Site Equipment	DCS-05	Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premises. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full overwrite of the drive to ensure that the erased drive is released to inventory for reuse and deployment, or securely stored until it can be destroyed.	ArcGIS Online cloud infrastructure providers have established policies and procedures for addressing off-site equipment aligning with ISO 27001 standards and NIST 800-88 Guidelines on Media Sanitization, which addresses the principle concern of ensuring that data is not unintentionally released.	X	X	A.8.1.1 A.8.1.2	NIST SP 800-53 R3 CM-8
Datacenter Security Policy	DCS-06	Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information.	Cloud infrastructure provider policies policy define and establish controls for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information. Access to media storage areas is restricted and audited. Access to all 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.	X	X	A.11.1.1 A.11.1.2	NIST SP 800-53 R3 PE-2 NIST SP 800-53 R3 PE-3 NIST SP 800-53 R3 PE-6
Datacenter Security Secure Area Authorization	DCS-07	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. Datacenter entrances are guarded 24x7x365 by security personnel and access is controlled through security personnel, authorized badges, locked doors and CCTV monitoring.	X		A.11.1.6	NIST SP 800-53 R3 PE-7 NIST SP 800-53 R3 PE-16
Datacenter Security Unauthorized Persons Entry	DCS-08	Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.	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.	X		A.11.2.5 8.1* (partial) A.12.1.2	NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MA-2 NIST SP 800-53 R3 PE-16

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	Supplier Relationship		Scope Applicability	
				Service Provider	Tenant / Consumer	ISO/IEC 27001:2013	FedRAMP --LOW IMPACT--
Datacenter Security User Access	DCS-09	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.	X		A.11.1.1	NIST SP 800-53 R3 PE-2 NIST SP 800-53 R3 PE-3 NIST SP 800-53 R3 PE-6
Encryption & Key Management Entitlement	EKM-01	Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.	Key management policies, procedures, and processes for ArcGIS Online align with FedRAMP Tailored Low requirements.	X	X	Annex A.10.1 A.10.1.1 A.10.1.2	
Encryption & Key Management Key Generation	EKM-02	Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.	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.	X		Clauses 5.2(c) 5.3(a) 5.3(b) 7.5.3(b) 7.5.3(d) 8.1 8.3 9.2(g) A.8.2.3 A.10.1.2 A.18.1.5	NIST SP 800-53 R3 SC-12 NIST SP 800-53 R3 SC-13
Encryption & Key Management Sensitive Data Protection	EKM-03	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.	ArcGIS Online utilizes encyrption in transit and at-rest by defaul. The customer's administrator can currently disable requiring encryption-in-transit via HTTPS (TLS) for customer data transmitted to and from their ArcGIS Online organization. All customer datasets updated since April 2018 are encrypted at rest with AES-256 bit encryption.	X		A.13.1.1 A.8.3.3 A.13.2.3 A.14.1.3 A.14.1.2 A.10.1.1 A.18.1.3 A.18.1.4	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-18 NIST SP 800-53 R3 IA-7 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SC-7 NIST SP 800-53 R3 SC-13
Encryption & Key Management Storage and Access	EKM-04	Platform and data-appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e., at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.	ArcGIS Online Key Management procedures align with FedRAMP Tailored Low requirements.	X	X	Annex A.10.1 A.10.1.1 A.10.1.2	

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	Supplier Relationship		Scope Applicability	
				Service Provider	Tenant / Consumer	ISO/IEC 27001:2013	FedRAMP --LOW IMPACT--
Governance and Risk Management Baseline Requirements	GRM-01	Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory, and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and authorized based on business needs.	As part of the overall FedRAMP accreditation, baseline security requirements are constantly being reviewed, improved and implemented as part of a Continuous Monitoring Program.	X		A.14.1.1 A.18.2.3	NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 SA-2 NIST SP 800-53 R3 SA-4
Governance and Risk Management Data Focus Risk Assessments	GRM-02	Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following: • Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure • Compliance with defined retention periods and end-of-life disposal requirements • Data classification and protection from unauthorized use, access, loss, destruction, and falsification	ArcGIS Online conducts regular risk assessment as part of alignment with FedRAMP 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.	X	X	Clauses 5.2(c) 5.3(a) 5.3(b) 6.1.2 6.1.2(a)(2) 6.1.3(b) 7.5.3(b) 7.5.3(d) 8.1 8.2 8.3 9.2(g) A.18.1.1 A.18.1.3 A.18.1.4 A.8.2.2	NIST SP 800-53 R3 CA-3 NIST SP 800-53 R3 RA-2 NIST SP 800-53 R3 RA-3 NIST SP 800-53 R3 SI-12
Governance and Risk Management Management Oversight	GRM-03	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.	X	X	Clause 7.2(a,b) A.7.2.1 A.7.2.2 A.9.2.5 A.18.2.2	NIST SP 800-53 R3 AT-2 NIST SP 800-53 R3 AT-3 NIST SP 800-53 R3 AT-4 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-5 NIST SP 800-53 R3 CA-6 NIST SP 800-53 R3 CA-7

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	Supplier Relationship		Scope Applicability	
				Service Provider	Tenant / Consumer	ISO/IEC 27001:2013	FedRAMP --LOW IMPACT--
Governance and Risk Management Management Program	GRM-04	An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business: • Risk management • Security policy • Organization of information security • Asset management • Human resources security • Physical and environmental security • Communications and operations management • Access control • Information systems acquisition, development, and maintenance	ArcGIS Online's ISMP is based upon NIST standards as part of FedRAMP accreditation. For international customers, a mapping of FedRAMP 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.	X	X	All in sections 4, 5, 6, 7, 8, 9, 10. A.6.1.1 A.13.2.4 A.6.1.3 A.6.1.4 A.18.2.1	
Governance and Risk Management Management Support/Involvement	GRM-05	Executive and line management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has been assigned.	Esri's security policies are signed and reviewed by executive management and disseminated to team members in alignment with the FedRAMP accreditation. Cloud infrastructure providers ensure policy and procedures are in alignment with ISO 27001 standards.	X		All in section 5 plus clauses 4.4 4.2(b) 6.1.2(a)(1) 6.2 6.2(a) 6.2(d) 7.1 7.4 9.3 10.2 7.2(a) 7.2(b) 7.2(c) 7.2(d) 7.3(b) 7.3(c)	NIST SP 800-53 R3 CM-1
Governance and Risk Management Policy	GRM-06	Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.	For more information, see GRM-05 above.	X	X	Clause 4.3 Clause 5 4.4 4.2(b) 6.1.2(a)(1) 6.2 6.2(a) 6.2(d) 7.1 7.4 9.3 10.2 7.2(a) 7.2(b) 7.2(c) 7.2(d) 7.3(b) 7.3(c) A5.1.1 A.7.2.2	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	Supplier Relationship		Scope Applicability	
				Service Provider	Tenant / Consumer	ISO/IEC 27001:2013	FedRAMP --LOW IMPACT--
Governance and Risk Management Policy Enforcement	GRM-07	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures.	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.	X	X	A7.2.3	NIST SP 800-53 R3 PL-4 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 PS-8
Governance and Risk Management Policy Impact on Risk Assessments	GRM-08	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that 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.	X	X	Clause 4.2.1 a, 4.2(b) 4.3 c, 4.3(a&b) 4.4 5.1(c) 5.1(d) 5.1(e) 5.1(f) 5.1(g) 5.1(h)	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CP-1
Governance and Risk Management Policy Reviews	GRM-09	The organization's business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.	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 FedRAMP 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.	X	X	Clause 8.1 A.5.1.2	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CP-1
Governance and Risk Management Risk Assessments	GRM-10	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).	Third party Risk Assessments are performed at least annually and a continuous monitoring plan is in place as specified by FedRAMP requirements for ArcGIS Online.	X	X	Clause 4.2(b), 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d)	NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 RA-1 NIST SP 800-53 R3 RA-2 NIST SP 800-53 R3 RA-3

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	Supplier Relationship		Scope Applicability	
				Service Provider	Tenant / Consumer	ISO/IEC 27001:2013	FedRAMP --LOW IMPACT--
Governance and Risk Management Risk Management Framework	GRM-11	Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and stakeholder approval.	The ArcGIS Online FedRAMP 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.	X	X	Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b)	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-6 NIST SP 800-53 R3 CA-7 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 RA-1 NIST SP 800-53 R3 RA-2 NIST SP 800-53 R3 RA-3
Human Resources Asset Returns	HRS-01	Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period.	Employees, contractors and third party users are 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.	X	X	A.8.1.1 A.8.1.2 A.8.1.4	NIST SP 800-53 R3 PS-4
Human Resources Background Screening	HRS-02	Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.	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.	X	X	A.7.1.1	NIST SP 800-53 R3 PS-2 NIST SP 800-53 R3 PS-3
Human Resources Employment Agreements	HRS-03	Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.	As part of the ArcGIS Online FedRAMP accreditation employees must sign a Rules of Behavior (RoB) 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.	X	X	A.13.2.4 A.7.1.2	NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 PS-2 NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 PS-7
Human Resources Employment Termination	HRS-04	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.	X	X	A.7.3.1	NIST SP 800-53 R3 PS-2 NIST SP 800-53 R3 PS-4 NIST SP 800-53 R3 PS-5 NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 PS-8

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	Supplier Relationship		Scope Applicability	
				Service Provider	Tenant / Consumer	ISO/IEC 27001:2013	FedRAMP --LOW IMPACT--
Human Resources Mobile Device Management	HRS-05	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring).	Esri has an established mobile device policy. Esri 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.	X	X	A.8.2.1 A.8.3.1 A.8.3.2 A.8.3.3 A.6.2.1 A.6.2.2 A.18.1.4	NIST SP 800-53 R3 AC-17 NIST SP 800-53 R3 AC-18 NIST SP 800-53 R3 AC-19 NIST SP 800-53 R3 MP-2 NIST SP 800-53 R3 MP-6
Human Resources Non-Disclosure Agreements	HRS-06	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.	X	X	A.13.2.4	NIST SP 800-53 R3 PL-4 NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 SA-9
Human Resources Roles / Responsibilities	HRS-07	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 ArcGIS Online System Security Plan. User roles and responsibilities are documented within the ArcGIS Online application documentation.	X	X	Clause 5.3 A.6.1.1 A.6.1.1	NIST SP 800-53 R3 PL-4 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 PS-2 NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 PS-7
Human Resources Technology Acceptable Use	HRS-08	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to corporate resources (i.e., BYOD) shall be considered and incorporated as appropriate.	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 Customers are responsible for ensuring users are aware of their own organization's acceptable use agreement. Organizations can choose to display a banner within their ArcGIS Online organization to communicate messages such as this. The Esri Employee Handbook specifies acceptable terms of use for all employees. For employees that work with ArcGIS Online, a separate Rules of Behavior (ROB) document is signed.	X	X	A.8.1.3	NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 AC-8 NIST SP 800-53 R3 AC-20 NIST SP 800-53 R3 PL-4
Human Resources Training / Awareness	HRS-09	A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	Annual security training is provided for ArcGIS Online employees.	X	X	Clause 7.2(a), 7.2(b) A.7.2.2	NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AT-2 NIST SP 800-53 R3 AT-3 NIST SP 800-53 R3 AT-4

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	Supplier Relationship		Scope Applicability	
				Service Provider	Tenant / Consumer	ISO/IEC 27001:2013	FedRAMP --LOW IMPACT--
Human Resources User Responsibility	HRS-10	All personnel shall be made aware of their roles and responsibilities for: • Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations. • Maintaining a safe and secure working environment	ArcGIS Online employees adhere to a rules of behavior policy outlining user responsibilities.	X	X	Clause 7.2(a), 7.2(b) A.7.2.2 A.9.3.1 A.11.2.8	NIST SP 800-53 R3 AT-2 NIST SP 800-53 R3 AT-3 NIST SP 800-53 R3 AT-4 NIST SP 800-53 R3 PL-4
Human Resources Workspace	HRS-11	Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions are disabled after an established period of inactivity.	Technical and procedural controls are part of ArcGIS Online's policies including areas such as defined session time-out requirements.	X	X	Clause 7.2(a), 7.2(b) A.7.2.2 A.11.1.5 A.9.3.1 A.11.2.8 A.11.2.9	NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 MP-2
Identity & Access Management Audit Tools Access	IAM-01	Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segregated and access restricted to prevent inappropriate disclosure and tampering of log data.	Access to information systems audit tools are restricted to authorized personnel within ArcGIS Online.	X	X		NIST SP 800-53 R3 AU-9
Identity & Access Management Credential Lifecycle / Provision Management	IAM-02	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following: • Procedures, supporting roles, and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships) • Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems) • Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant)) • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Authentication, authorization, and accounting (AAA) rules for access to data and sessions (e.g., encryption and strong/multi-	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.	X		A.9.1.1 A.9.2.1, A.9.2.2 A.9.2.5 A.9.1.2 A.9.4.1	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-7 NIST SP 800-53 R3 AC-14 NIST SP 800-53 R3 IA-1
Identity & Access Management Diagnostic / Configuration Ports Access	IAM-03	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.	X	X	A.13.1.1 A.9.1.1 A.9.4.4	NIST SP 800-53 R3 CM-7 NIST SP 800-53 R3 MA-4 NIST SP 800-53 R3 MA-5

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	Supplier Relationship		Scope Applicability	
				Service Provider	Tenant / Consumer	ISO/IEC 27001:2013	FedRAMP --LOW IMPACT--
Identity & Access Management Policies and Procedures	IAM-04	Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.	Customers have the responsibility of managing access and privilege levels to their ArcGIS Online organization. The use of Enterprise Logins (using SAML 2.0) to identity federation and the use of custom roles in ArcGIS Online to granularly define privileges are recommended best practices. Less than 10 ArcGIS Online Administrators are responsible for managing ArcGIS instances and connect using X.509 certificates. Cloud infrastructure providers have controls in place for limiting access that align with ISO 27001 and FedRAMP Moderate requirements.	X		Annex A.9.2 A.9.2.1 A.9.2.2 A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6	
Identity & Access Management Segregation of Duties	IAM-05	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.	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	X		A.6.1.2	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 AU-2 NIST SP 800-53 R3 AU-6
Identity & Access Management Source Code Access Restriction	IAM-06	Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.	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.	X		Clause 5.2(c) 5.3(a), 5.3(b), 7.5.3(b) 7.5.3(d) 8.1, 8.3 9.2(g) A.9.4.5 A.18.1.3	
Identity & Access Management Third Party Access	IAM-07	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.	X	X	A.9.2.6 A.9.1.1 A.9.2.1, A.9.2.2 A.9.2.5	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 IA-1

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	Supplier Relationship		Scope Applicability	
				Service Provider	Tenant / Consumer	ISO/IEC 27001:2013	FedRAMP --LOW IMPACT--
Identity & Access Management Trusted Sources	IAM-08	Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.	Customers have the responsibility of managing access and privilege levels to their ArcGIS Online organization. The use of Enterprise Logins (using SAML 2.0) for identity federation to authenticate and the use of custom roles in ArcGIS Online to granularly define privileges are recommended best practices. Less than 10 Esri employees, that are specialized ArcGIS Online administrators, utilizing X.509 certificates for authentication, have access to customer data.	X	X	Annex A.9.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.1, A.9.4.2, A.9.4.3, A.9.4.5	
Identity & Access Management User Access Authorization	IAM-09	Provisioning user access (e.g., employees, contractors, customers (tenants), business partners, and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, provider shall inform customer (tenant) of this user access, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Less than 10 Esri employees, that are specialized ArcGIS Online administrators, utilizing X.509 certificates for authentication, have access to customer data.	X	X	A.9.2.1, A.9.2.2 A.9.2.3 A.9.1.2 A.9.4.1	NIST SP 800-53 R3 AC-3 NIST SP 800-53 R3 IA-2 NIST SP 800-53 R3 IA-2 (1) NIST SP 800-53 R3 IA-4 NIST SP 800-53 R3 IA-5 NIST SP 800-53 R3 IA-5 (1) NIST SP 800-53 R3 IA-8 NIST SP 800-53 R3 MA-5 NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 SA-7
Identity & Access Management User Access Reviews	IAM-10	User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow established user access policies and procedures.	Customers are responsible for reviewing their user access to their ArcGIS Online organization at defined intervals. The use of Enterprise Logins (using SAML 2.0) is a best practice recommendations to ensure built-in accounts are minimally used. In alignment with FedRAMP 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.	X	X	A.9.2.5	NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 AU-6 NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 PS-7
Identity & Access Management User Access Revocation	IAM-11	Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change, or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Customers are responsible for managing access to the applications and services customers host on ArcGIS Online. The use of Enterprise Logins (using SAML 2.0) minimizes the requirements for built-in ArcGIS Online accounts and would ensure that removal of a customer user from their Active Directory (or LDAP) would ensure access to ArcGIS Online was also no longer possible.	X		Annex A A.9.2.6 A.9.1.1 A.9.2.1, A.9.2.2 A.9.2.3	NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 PS-4 NIST SP 800-53 R3 PS-5

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	Supplier Relationship		Scope Applicability	
				Service Provider	Tenant / Consumer	ISO/IEC 27001:2013	FedRAMP --LOW IMPACT--
Identity & Access Management User ID Credentials	IAM-12	Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures: • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)	Organizations should utilize ArcGIS Online Enterprise Logins to meet all of their organizations username and password management requirements and for adherence to FedRAMP and ISO 27001 security requirements. Further information concerning ArcGIS Online Enterprise Logins may be found at: http://doc.arcgis.com/en/arcgis-online/administer/enterprise-logins.htm If an Identity Provider (IdP) is not available. ArcGIS Online enabled Administrators to implement a custom password policy for their ArcGIS Online organization. Other than User ID lockouts which are fixed settings, password policies can be customized to meet these requirements or the specific requirements outlined in the customer's policies. For more info on setting a custom password policy, see: https://doc.arcgis.com/en/arcgis-online/administer/configure-security.htm	X	X	A.9.2.6 A.9.1.1 A.9.2.1, A.9.2.2 A.9.2.4 A.9.2.5 A.9.4.2	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 AC-3 NIST SP 800-53 R3 AU-2 NIST SP 800-53 R3 AU-11 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IA-2 NIST SP 800-53 R3 IA-2 (1) NIST SP 800-53 R3 IA-5 NIST SP 800-53 R3 IA-5 (1) NIST SP 800-53 R3 IA-6 NIST SP 800-53 R3 IA-8
Identity & Access Management Utility Programs Access	IAM-13	Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.	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.	X	X	A.9.1.2 Deleted A.9.4.4	NIST SP 800-53 R3 CM-7
Infrastructure & Virtualization Security Audit Logging / Intrusion Detection	IVS-01	Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.	Access to logs is restricted as defined by policy, and logs are reviewed on a regular basis in alignment with FedRAMP Tailored Low requirements.	X		A.12.4.1 A.12.4.1 A.12.4.2, A.12.4.3 A.12.4.3 A.12.4.1 A.9.2.3 A.9.4.4 A.9.4.1 A.16.1.2 A.16.1.7 A.18.2.3 A.18.1.3	NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 AU-2 NIST SP 800-53 R3 AU-3 NIST SP 800-53 R3 AU-4 NIST SP 800-53 R3 AU-5 NIST SP 800-53 R3 AU-6 NIST SP 800-53 R3 AU-9 NIST SP 800-53 R3 AU-11 NIST SP 800-53 R3 AU-12 NIST SP 800-53 R3 PE-2 NIST SP 800-53 R3 PE-3

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	Supplier Relationship		Scope Applicability	
				Service Provider	Tenant / Consumer	ISO/IEC 27001:2013	FedRAMP --LOW IMPACT--
Infrastructure & Virtualization Security Change Detection	IVS-02	The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g., dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g., portals or alerts).	Base virtual machine images are provided by the cloud infrastructure provider and refreshed as part of new releases. Console interfaces provide status information for each virtual machine.	X		Annex A.12.1.2 A.12.4, A.12.4.1, A.12.4.2, A.12.4.3, A.12.6.1, A.12.6.2, A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7	
Infrastructure & Virtualization Security Clock Synchronization	IVS-03	A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.	In order to both increase the security of ArcGIS Online, and to provide accurate reporting detail in event logging and monitoring processes and records, 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 the ArcGIS Online systems.	X		A.12.4.1 A.12.4.4	NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 AU-8
Infrastructure & Virtualization Security Information System Documentation	IVS-04	The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.	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.	X	X	A.12.1.3	NIST SP 800-53 R3 SA-4
Infrastructure & Virtualization Security Vulnerability Management	IVS-05	Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g., virtualization aware).	Cloud infrastructure providers virtualization technologies are regularly evaluated internally and by independent assessments.	X		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)	
Infrastructure & Virtualization Security Network Security	IVS-06	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, ports, and by compensating controls.	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.	X	X	A.13.1.1 A.13.1.2 A.14.1.2 A.12.4.1 A.9.1.2 A.13.1.3 A.18.1.4	NIST SP 800-53 R3 CM-7 NIST SP 800-53 R3 SC-7 NIST SP 800-53 R3 SC-20 (1)
Infrastructure & Virtualization Security OS Hardening and Base Controls	IVS-07	Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.	ArcGIS Online uses a standard image for all instances and this includes the deployment of anti-virus on customer-facing instances. Logging within ArcGIS Online aligns with FedRAMP Tailored Low requirements.	X	X	Annex A.12.1.4 A.12.2.1 A.12.4.1 A.12.6.1	

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	Supplier Relationship		Scope Applicability	
				Service Provider	Tenant / Consumer	ISO/IEC 27001:2013	FedRAMP --LOW IMPACT--
Infrastructure & Virtualization Security Production / Non-Production Environments	IVS-08	Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.	ArcGIS Online utilizes separate production and non-production environments.	X		A.12.1.4 A.14.2.9 A.9.1.1 8.1,partial, A.14.2.2 8.1,partial, A.14.2.3 8.1,partial, A.14.2.4	
Infrastructure & Virtualization Security Segmentation	IVS-09	Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed, and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations: • Established policies and procedures • Isolation of business critical assets and/or sensitive user data, and sessions that mandate stronger internal controls and high levels of assurance • Compliance with legal, statutory, and regulatory compliance obligations	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.	X	X	A.13.1.3 A.9.4.1 A.18.1.4	NIST SP 800-53 R3 SC-7
Infrastructure & Virtualization Security VM Security - Data Protection	IVS-10	Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from production-level networks for such migrations.	Customers can migrate data to ArcGIS Online via HTTPS for encrypted communitcation. Customers can also deploy a separate non-production ArcGIS Online organization for initial data migrating /testing efforts.	X		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)	
Infrastructure & Virtualization Security Hypervisor Hardening	IVS-11	Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).	ArcGIS Online's cloud infrastructure providers use a concept of least privilege for assigning access to all functions. These technical and procedural controls align with ISO 27001 and FedRAMP Moderate requirements.	X		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d)	
Infrastructure & Virtualization Security Wireless Security	IVS-12	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following: • Perimeter firewalls implemented and configured to restrict unauthorized traffic • Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings) • 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 which includes monitoring. Access from a wireless network on a customer premise to the ArcGIS Online environment must be secured by the customer.	X	X	A.8.1.1 A.8.1.2 A.8.1.3 A.11.2.1 A.11.2.4 A.13.1.1 A.13.1.2 A.13.2.1 A.8.3.3 A.12.4.1 A.9.2.1, A.9.2.2 A.13.1.3 A.10.1.1 A.10.1.2	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-18 NIST SP 800-53 R3 CM-6 NIST SP 800-53 R3 SC-7

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	Supplier Relationship		Scope Applicability	
				Service Provider	Tenant / Consumer	ISO/IEC 27001:2013	FedRAMP --LOW IMPACT--
Infrastructure & Virtualization Security Network Architecture	IVS-13	Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.	ArcGIS Online's cloud infrastructure providers are subjected to regular internal and external testing. In addition their security controls are reviewed regularly by independent auditors and align with ISO 27001 and FedRAMP Moderate requirements.	X	X		
Interoperability & Portability APIs	IPY-01	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	The ArcGIS Online API is publically available. For more information see: https://doc.arcgis.com/en/arcgis-online/reference/develop-with-agol.htm	X		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)	
Interoperability & Portability Data Request	IPY-02	All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files).	Customers retain ownership of their data at all times and can export their data from ArcGIS Online in standard formats at any time.	X		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2)	
Interoperability & Portability Policy & Legal	IPY-03	Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence.	The ArcGIS Online REST API is publically available. For more information see: https://doc.arcgis.com/en/arcgis-online/reference/develop-with-agol.htm . Legal aspects are addressed as part of the Terms of Service at: http://www.esri.com/legal/pdfs/mla_e204_e300/english#Addendum_3	X	X	Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d)	
Interoperability & Portability Standardized Network Protocols	IPY-04	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.	Customer's retain ownership of their data at all times and are responsible for the import and export of that data into their ArcGIS Organization. Customer can require HTTPS for their ArcGIS Online organization to ensure data is sent over encrypted means and they must be authenticated to ArcGIS Online to perform this function.	X		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1),	
Interoperability & Portability Virtualization	IPY-05	The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use and all solution-specific virtualization hooks available for customer review.	ArcGIS Online's cloud infrastructure providers have virtualization platforms that are reviewed regularly by independent audits and align with ISO 27001 and FedRAMP Moderate requirements. The virtual machine images are not exposed/provided to customers so the utilization of OVF is not appliable.	X		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d)	

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	Supplier Relationship		Scope Applicability	
				Service Provider	Tenant / Consumer	ISO/IEC 27001:2013	FedRAMP --LOW IMPACT--
Mobile Security Anti-Malware	MOS-01	Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	X		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2)	
Mobile Security Application Stores	MOS-02	A documented list of approved application stores has been defined as acceptable for mobile devices accessing or storing provider managed data.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	X		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2)	
Mobile Security Approved Applications	MOS-03	The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	X		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d)	
Mobile Security Approved Software for BYOD	MOS-04	The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	X		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)	
Mobile Security Awareness and Training	MOS-05	The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and training program.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	X		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d)	

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	Supplier Relationship		Scope Applicability	
				Service Provider	Tenant / Consumer	ISO/IEC 27001:2013	FedRAMP --LOW IMPACT--
Mobile Security Cloud Based Services	MOS-06	All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	X	X	Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)	
Mobile Security Compatibility	MOS-07	The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	X		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d)	
Mobile Security Device Eligibility	MOS-08	The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	X		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1),	
Mobile Security Device Inventory	MOS-09	An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD)) will be included for each device in the inventory.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	X		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1),	
Mobile Security Device Management	MOS-10	A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	X		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1),	
Mobile Security Encryption	MOS-11	The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices, and shall be enforced through technology controls.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	X		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2)	

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	Supplier Relationship		Scope Applicability	
				Service Provider	Tenant / Consumer	ISO/IEC 27001:2013	FedRAMP --LOW IMPACT--
Mobile Security Jailbreaking and Rooting	MOS-12	The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting) and shall enforce the prohibition through detective and preventative controls on the device or through a centralized device management system (e.g., mobile device management).	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	X		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1),	
Mobile Security Legal	MOS-13	The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the expectations regarding the loss of non-company data in the case that a wipe of the device is required.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	X	X	Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2)	
Mobile Security Lockout Screen	MOS-14	BYOD and/or company-owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	X	X	Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)	
Mobile Security Operating Systems	MOS-15	Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	X	X	Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)	
Mobile Security Passwords	MOS-16	Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	X	X	Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2)	
Mobile Security Policy	MOS-17	The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	X	X	Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)	

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	Supplier Relationship		Scope Applicability	
				Service Provider	Tenant / Consumer	ISO/IEC 27001:2013	FedRAMP --LOW IMPACT--
Mobile Security Remote Wipe	MOS-18	All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	X	X	Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)	
Mobile Security Security Patches	MOS-19	Mobile devices connecting to corporate networks, or storing and accessing company information, shall allow for remote software version/patch validation. All mobile devices shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel shall be able to perform these updates remotely.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	X	X	Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1),	
Mobile Security Users	MOS-20	The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	X	X	Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)	
Security Incident Management, E-Discovery, & Cloud Forensics Contact / Authority Maintenance	SEF-01	Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.	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.	X	X	A.6.1.3 A.6.1.4	NIST SP 800-53 R3 IR-6 NIST SP 800-53 R3 SI-5
Security Incident Management, E-Discovery, & Cloud Forensics Incident Management	SEF-02	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.	Incident management is delineated within ArcGIS Online's Incident Response Plan documentation aligning with FedRAMP requirements.	X	X	Clause 5.3 (a), 5.3 (b), 7.5.3(b), 5.2 (c), 7.5.3(d), 8.1, 8.3, 9.2(g), Annex A.16.1.1 A.16.1.2	NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 IR-2 NIST SP 800-53 R3 IR-4 NIST SP 800-53 R3 IR-5 NIST SP 800-53 R3 IR-6 NIST SP 800-53 R3 IR-7

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	Supplier Relationship		Scope Applicability	
				Service Provider	Tenant / Consumer	ISO/IEC 27001:2013	FedRAMP --LOW IMPACT--
Security Incident Management, E-Discovery, & Cloud Forensics Incident Reporting	SEF-03	Workforce personnel and external business relationships shall be informed of their responsibilities and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.	ArcGIS Online's incident response program, plans and procedures have been developed in alignment with FedRAMP requirements. Customers can inform the security team directly of any suspected information security event through the 'Report a Security Concern' page on the Trust.ArcGIS.com site at: http://doc.arcgis.com/en/trust/security-concern/	X	X	Clause 5.2 (c), 5.3 (a), 5.3 (b), 7.2(a), 7.2(b), 7.2(c), 7.2(d), 7.3(b), 7.3(c) 7.5.3(b), 7.5.3(d), 8.1, 8.3, 9.2(g) Annex A.6.1.1 A.7.2.1, A.7.2.2, A.16.1.2, A.16.1.3, A.16.1.1	NIST SP 800-53 R3 IR-2 NIST SP 800-53 R3 IR-6 NIST SP 800-53 R3 IR-7 NIST SP 800-53 R3 SI-5
Security Incident Management, E-Discovery, & Cloud Forensics Incident Response Legal Preparation	SEF-04	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.	ArcGIS Online's incident response program, plans and procedures have been developed in alignment with FedRAMP requirements.	X	X	Clause 5.2 (c), 5.3 (a), 5.3 (b), 7.2(a), 7.2(b), 7.2(c), 7.2(d), 7.3(b), 7.3(c) 7.5.3(b), 7.5.3(d), 8.1, 8.3, 9.2(g) Annex A.7.2.2, A.7.2.3, A.16.1.7, A.18.1.3	NIST SP 800-53 R3 AU-6 NIST SP 800-53 R3 AU-9 NIST SP 800-53 R3 AU-11 NIST SP 800-53 R3 IR-5 NIST SP 800-53 R3 IR-7 NIST SP 800-53 R3 IR-8
Security Incident Management, E-Discovery, & Cloud Forensics Incident Response Metrics	SEF-05	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.	X	X	A.16.1.6	NIST SP 800-53 R3 IR-4 NIST SP 800-53 R3 IR-5 NIST SP 800-53 R3 IR-8
Supply Chain Management, Transparency, and Accountability Data Quality and Integrity	STA-01	Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.	ArcGIS Online uses cloud infrastructure providers whose risk management practices align with ISO 27001 and FedRAMP Moderate requirements.	X		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d)	

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	Supplier Relationship		Scope Applicability	
				Service Provider	Tenant / Consumer	ISO/IEC 27001:2013	FedRAMP --LOW IMPACT--
Supply Chain Management, Transparency, and Accountability Incident Reporting	STA-02	The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals).	General site information for ArcGIS Online is available via the Status page of the Trust.ArcGIS.com website. Informaiton about customer specific incidents can be viewed via the MyEsri Support portal.	X		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d)	
Supply Chain Management, Transparency, and Accountability Network / Infrastructure Services	STA-03	Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.	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.	X	X	A.15.1.2 A.13.1.2	NIST SP 800-53 R3 CA-3 NIST SP 800-53 R3 SA-9
Supply Chain Management, Transparency, and Accountability Provider Internal Assessments	STA-04	The provider shall perform annual internal assessments of conformance to, and effectiveness of, its policies, procedures, and supporting measures and metrics.	As part of FedRAMP Tailored Low compliance, ArcGIS Online implements a robust continuous monitoring program to monitor risk which includes regular internal assessments.	X		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d)	

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	Supplier Relationship		Scope Applicability	
				Service Provider	Tenant / Consumer	ISO/IEC 27001:2013	FedRAMP --LOW IMPACT--
Supply Chain Management, Transparency, and Accountability Supply Chain Agreements	STA-05	Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations) • Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships • Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts • Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain) • Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed • Expiration of the business relationship and treatment of customer (tenant) data impacted • Customer (tenant) service-to-service application (API) and data interoperability and portability requirements for application	Third party agreements are reviewed by Esri Contracts and/or Legal Counsel as appropriate.	X	X	A.15.1.2, 8.1* partial, A.13.2.2, A.9.4.1 A.10.1.1	NIST SP 800-53 R3 CA-3 NIST SP 800-53 R3 PS-7 NIST SP 800-53 R3 SA-6 NIST SP 800-53 R3 SA-7 NIST SP 800-53 R3 SA-9
Supply Chain Management, Transparency, and Accountability Supply Chain Governance Reviews	STA-06	Providers shall review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.	ArcGIS Online uses cloud infrastructure providers whose risk management practices align with stringent ISO 27001 and FedRAMP Moderate requirements.	X		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1)	
Supply Chain Management, Transparency, and Accountability Supply Chain Metrics	STA-07	Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews shall be performed at least annually and identify any non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.	See STA-03 for more information.	X		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3)	

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	Supplier Relationship		Scope Applicability	
				Service Provider	Tenant / Consumer	ISO/IEC 27001:2013	FedRAMP --LOW IMPACT--
Supply Chain Management, Transparency, and Accountability Third Party Assessment	STA-08	Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review shall include all partners/third party-providers upon which their information supply chain depends on.	ArcGIS Online uses cloud infrastructure providers whose risk management practices align with stringent ISO 27001 and FedRAMP Moderate requirements.	X		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)	
Supply Chain Management, Transparency, and Accountability Third Party Audits	STA-09	Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.	ArcGIS Online uses cloud infrastructure providers whose risk management practices align with stringent ISO 27001 and FedRAMP Moderate requirements.	X		A.15.1.2 8.1* partial, 8.1* partial, A.15.2.1 A.13.1.2	NIST SP 800-53 R3 CA-3 NIST SP 800-53 R3 SA-9 NIST SP 800-53 R3 SC-7
Threat and Vulnerability Management Anti-Virus / Malicious Software	TVM-01	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	A number of key security parameters are monitored to identify potentially malicious activity on the systems which includes the use anti-malware software on systems accepting customer datasets/information. Cloud infrastructure provider anti-virus controls align with ISO 27001 requirements.	X	X	A.12.2.1	NIST SP 800-53 R3 SC-5 NIST SP 800-53 R3 SI-3 NIST SP 800-53 R3 SI-5
Threat and Vulnerability Management Vulnerability / Patch Management	TVM-02	Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	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.	X		8.1*partial, A.14.2.2, 8.1*partial, A.14.2.3 A.12.6.1	NIST SP 800-53 R3 CM-4 NIST SP 800-53 R3 RA-5 NIST SP 800-53 R3 SI-1 NIST SP 800-53 R3 SI-2 NIST SP 800-53 R3 SI-5
Threat and Vulnerability Management Mobile Code	TVM-03	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	ArcGIS Online does not require installable mobile code such as MS ActiveX, Adobe Flash, and MS Silverlight.	X	X	A.12.2.1	