ArcGIS Online
Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire (CAIQ) 3.1 - July 2021

Attached are Esri's self-assessment answers to the Cloud Security Alliance (CSA) Consensus Assessment Initiative Questionnaire (CAIQ) 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 310 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 began providing answers for the CSA CCM (133 questions) in 2013, and now utilize the more extensive (CAIQ v3.1) with 310 questions/answers.

ArcGIS Online is audited annually by a 3rd party assessor to ensure alignment with its 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: https://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: https://downloads.esri.com/resources/enterprisegis/AGOL_CSA_CAIQ.pdf

For a more lightweight set of answers, a basic overview of ArcGIS Online security (2-page flyer) is available within the Trust Center documents. Some basic, recurring customers questions include:

- *Where is my data hosted?* Within AWS and MS Azure datacenters on US Soil by default, new organizations can choose to have their data stored in regions outside the US, such as the EU or AP Regions.
- *Is my data encrypted at rest and in transit?* Yes, organizations use HTTPS w/TLS 1.2 for in-transit and AES-256 at rest.
- *Is my data backed up?* Customers are responsible for backing up their datasets.
- *Can I do security tests against ArcGIS Online?* Yes, however a Security Assessment Agreement (SAA) must be completed first.
- *Are my files scanned with Anti-virus?* Yes – Files containing malicious code are rejected from upload.
- *What privacy assurance is in place?* ArcGIS Online is both GDPR and CCPA aligned.

For any questions/concerns/feedback please contact Esri's Software Security & Privacy Team at:
SoftwareSecurity@Esri.com

Control Domain	Question ID	Control Specification	Consensus Assessment Questions	Yes	No	N/A	FedRAMP Low 800-53	ISO 27001:2013	Notes
Application & Interface Security *Application Security*	AIS-01.1	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.	Do you use industry standards (i.e. OWASP Software Assurance Maturity Model, ISO 27034) to build in security for your Systems/Software Development Lifecycle (SDLC)?	X			SC-5 SC-6 SC-7 SC-12 SC-13 SC-14	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	Esri utilizes the Building Security In Maturity Model (BSIMM) as the backbone to measure its efforts to immerse security throughout the development life cycle in the most effective manner for its products. ArcGIS Online is FedRAMP Tailored Low authorized and therefore also aligns with NIST standards. Please see our Secure Development Lifecycle Overview on within the ArcGIS Trust Center documents https://trust.arcgis.com for more information.
	AIS-01.2		Do you use an automated source code analysis tool to detect security defects in code prior to production?	X					Esri utilizes the Building Security In Maturity Model (BSIMM) as the backbone to measure its efforts to immerse security throughout the development life cycle in the most effective manner for its products. ArcGIS Online is FedRAMP Tailored Low authorized and therefore also aligns with NIST standards. Please see our Secure Development Lifecycle Overview on within the ArcGIS Trust Center documents https://trust.arcgis.com for more information.
	AIS-01.3		Do you use manual source-code analysis to detect security defects in code prior to production?		X				Manual spot checks are performed on code based on risk and including ad-hoc third party validation efforts.
	AIS-01.4		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	X					
	AIS-01.5		(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	X					Priority of addressing vulnerabilities in alignment with FedRAMP Tailored Low requirements.
Application & Interface Security *Customer Access Requirements*	AIS-02.1	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?	X			CA-1 CA-2 CA-2 (1) CA-5 CA-6	A9.1.1.	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 at: http://www.esri.com/legal/pdfs/mla_e204_e300/english#Addendum_3 and Privacy policy @ http://www.esri.com/legal/privacyarcgis. ArcGIS Online maintains a FedRAMP Tailored Low security authorization through the US Government and utilizes cloud infrastructure providers that are ISO 27001 compliant. It aligns with GDPR and CCPA for privacy assurance. Additional information concerning the security and privacy of ArcGIS Online may be found within the Trust.ArcGIS.com website.
	AIS- 02.2		Are all requirements and trust levels for customers' access defined and documented?	X					See response above.
Application & Interface Security *Data Integrity*	AIS-03.1	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.	Does your data management policies and procedures require audits to verify data input and output integrity routines?	X			SI-2 SI-3	A13.2.1, A13.2.2, A9.1.1, A9.4.1, A10.1.1 A18.1.4	Data logging in alignment with NIST standards
	AIS-03.2		Are data input and output integrity routines (i.e. MD5/SHA checksums) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	X					HTTPS (TLS 1.2) is enforced for ArcGIS Online organizations 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.
Application & Interface Security *Data Security / Integrity*	AIS-04.1	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, alternation, or destruction.	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	X			AC-1 SC-1 SC-13	A13.2.1, A13.2.2, A9.1.1, A9.4.1, A10.1.1 A18.1.4	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 its 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.

Control Domain	Question ID	Control Specification	Consensus Assessment Questions	Yes	No	N/A	FedRAMP Low 800-53	ISO 27001:2013	Notes
Audit Assurance & Compliance *Audit Planning*	AAC-01.1	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.	Do you develop and maintain an agreed upon audit plan (e.g., scope, objective, frequency, resources,etc.) for reviewing the efficiency and effectiveness of implemented security controls?	X			CA-2 CA-2 (1) CA-7	Clauses 4.3(a), 4.3(b), 5.1(e), 5.1(f), 6.2(e), 9.1, 9.1(e),	
	AAC-01.2		Does your audit program take into account effectiveness of implementation of security operations?	X					
Audit Assurance & Compliance *Independent Audits*	AAC-02.1	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.	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	X			CA-1 CA-2 CA-2 (1) CA-6 RA-5	Clauses 4.3(a), 4.3(b), 5.1(e), 5.1(f), 9.1, 9.2, 9.3(f), A18.2.1	ArcGIS Online has a FedRAMP-Tailored LOW ATO. An annual security assessment is performed by a 3rd party organization. A summary assessment report can be obtained with an NDA in place
	AAC-02.2		Do you conduct network penetration tests of your cloud service infrastructure at least annually?	X					ArcGIS Online solution is annually assessed/audited by a 3rd party assessor as per FedRAMP-Tailored LOW requirements
	AAC-02.3		Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	X					Penetration testing is not required for alignment with FedRAMP-Tailored Low, however, pentesting is performed ad-hoc by a 3rd party as necessary.
	AAC-02.4		Do you conduct internal audits at least annually?	X					ArcGIS Online solution is annually assessed/audited by a 3rd party assessor as per FedRAMP-Tailored LOW requirements
	AAC-02.5		Do you conduct independent audits at least annually?	X					ArcGIS Online solution is annually assessed/audited by a 3rd party assessor as per FedRAMP-Tailored LOW requirements
	AAC-02.6		Are the results of the penetration tests available to tenants at their request?	X					3rd party assessment results can be shared under NDA.
	AAC-02.7		Are the results of internal and external audits available to tenants at their request?	X					The results from the annual FedRAMP Security assessments are available in a summary report. This can be provided to clients upon signing an NDA.
Audit Assurance & Compliance *Information System Regulatory Mapping*	AAC-03.1	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.	Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	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),	All customer data in ArcGIS Online is encrypted at rest. Also, every customer organization has their own logically separated database for hosted feature service data.
Business Continuity Management & Operational Resilience *Business Continuity Planning*	BCR-01.1	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,	Does your organization have a plan or framework for business continuity management or disaster recovery management?	X			CP-1 CP-2 CP-3 CP-4 CP-9 CP-10	Clause 5.1(h) A.17.1.2 A.17.1.2	
	BCR-01.2		Do you have more than one provider for each service you depend on?		X				ArcGIS Online operation with two Cloud Service Providers AWS & Microsoft Azure and the CSPs operation in multiple Availability Zones as well as regions for redundancy. Some services are only available from one of the providers.
	BCR-01.3		Do you provide a disaster recovery capability?	X					ArcGIS Online systems run active-active across datacenters in a common region, and if those multiple datacenters experience a disaster, the system can be recovered in remote datacenter locations.
	BCR-01.4		Do you monitor service continuity with upstream providers in the event of provider failure?	X					
	BCR-01.5		Do you provide access to operational redundancy reports, including the services you rely on?	X					Contingency Plan reviewed by third party for compliance with FedRAMP Tailored Low requirements. Availability information posted to status page of ArcGIS Trust Center.
	BCR-01.6		Do you provide a tenant-triggered failover option?		X				Esri manages failovers

Control Domain	Question ID	Control Specification	Consensus Assessment Questions	Yes	No	N/A	FedRAMP Low 800-53	ISO 27001:2013	Notes
	BCR-01.7	and responsibilities • Detailed recovery procedures, manual work-around, and reference information • Method for plan invocation	Do you share your business continuity and redundancy plans with your tenants?		X				Business continuity plan is not shared publicly. All ArcGIS Online systems are redundant spanning multiple datacenters
Business Continuity Management & Operational Resilience *Business Continuity Testing*	BCR-02.1	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.	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?		X		CP-2 CP-3 CP-4	A17.3.1	Esri's business continuity plan is not tested at planned intervals. Esri maintains a detailed Contingency Plan for ArcGIS Online that involves the following: roles and responsibilities of key personnel, notification and escalation procedures, recovery plans, recovery time objective (RTO) and recovery point objective (RPO) and a clearly defined communication process. The ArcGIS Online Contingency Plan is tested at least annually.
Business Continuity Management & Operational Resilience *Power / Telecommunications*	BCR-03.1	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.	Does your organization adhere to any international or industry standards when it comes to securing, monitoring, maintaining and testing of datacenter utilities services and environmental conditions?	X			PE-1 PE-13 PE-13 (1) PE-13 (2) PE-13 (3	A11.2.2, A11.2.3	ArcGIS Online is FedRAMP Tailored Low authorized and therefore also aligns with NIST standards.
	BCR-03.2		Has your organization implemented environmental controls, fail-over mechanisms or other redundancies to secure utility services and mitigate environmental conditions?	X					
Business Continuity Management & Operational Resilience Documentation	BCR-04.1	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	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	X			CP-9 CP-10 SA-5	Clause 9.2(g)	Authorized administrators who have been read into the ArcGIS Online FedRAMP program have access architectural and user guides for administration purposes.
Business Continuity Management & Operational Resilience *Environmental Risks*	BCR-05.1	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.	Is physical damage anticipated and are countermeasures included in the design of physical protections?	X			PE-1 PE-13 PE-14 PE-15	A11.1.4, A11.2.1	ArcGIS Online Cloud infrastructure providers align with ISO 27001 and FedRAMP- moderate requirements. ArcGIS Online layer's it security controls on top of the CSP infrastructure and is authorized as a FedRAMP Tailored Low SaaS offering overall.

Control Domain	Question ID	Control Specification	Consensus Assessment Questions	Yes	No	N/A	FedRAMP Low 800-53	ISO 27001:2013	Notes
Business Continuity Management & Operational Resilience *Equipment Location*	BCR-06.1	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.	Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?		X		PE-1 PE-14 PE-15	A11.2.1	See MS Azure and Amazon Web Services security documentation for details
Business Continuity Management & Operational Resilience *Equipment Maintenance*	BCR-07.1	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.	Do you have documented policies, procedures and supporting business processes for equipment and datacenter maintenance?	X			MA-2 MA-4 MA-5	A11.2.4	Esri leverages AWS and Azure datacenter documentation
	BCR-07.2		Do you have an equipment and datacenter maintenance routine or plan?	X					Esri leverages the plan of AWS and Azure datacenters
Business Continuity Management & Operational Resilience *Equipment Power Failures*	BCR-08.1	Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific business impact assessment.	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	X			PE-1 PE-12 PE-13 PE-14	A.11.2.2, A.11.2.3, A.11.2.4	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.
Business Continuity Management & Operational Resilience *Impact Analysis*	BCR-09.1	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	Do you use industry standards and frameworks to determine the impact of any disruption to your organization (i.e. criticality of services and recovery priorities, disruption tolerance, RPO and RTO etc) ?	X			CP-1 CP-2 RA-3	A.17.1.1 A.17.1.2	ArcGIS Online Buisness Impact Assessment and updated annually in alignment with FedRAMP standards..
	BCR-09.2		Does your organization conduct impact analysis pertaining to possible disruptions to the cloud service?	X					ArcGIS Online Buisness Impact Assessment and updated annually.
Business Continuity Management & Operational Resilience *Policy*	BCR-10.1	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.	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	X			CM-2 CM-4 CM-6 MA-4 SA-3 SA-4 SA-5	Clause 5.1(h) A.6.1.1 A.7.2.1 A.7.2.2 A.12.1.1	ArcGIS Online has a detailed Roles and Responsibilities Matrix as part of the System Security Plan (SSP) with supporting security training materials. Esri employees accessing ArcGIS Online must sign a Rules of Behavior (RoB) that outlines employee technical and organizational responsibilities related to access and use.
Business Continuity Management & Operational Resilience *Retention Policy*	BCR-11.1	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.	Do you have technical capabilities to enforce tenant data retention policies?	X			CP-2 CP-9	Clauses 9.2(g) 7.5.3(b)	Customers have complete ownership of their data at all times. Customer datasets are deleted within 60 days of contract termination unless otherwise specified by the customer.
	BCR-11.2		Do you have documented policies and procedures demonstrating adherence to data retention periods as per legal, statutory or regulatory compliance requirements?	X				5.2 (c) 7.5.3(d) 5.3(a)	Customers have complete ownership of their data at all times. Customer datasets are deleted within 60 days of contract termination unless otherwise specified by the customer.
	BCR-11.3		Have you implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	X				5.3(b) 8.1 8.3	ArcGIS Online uses cloud infrastructure providers whose datacenters comply with industry standards (such as ISO 27001) for physical security and availability.
	BCR-11.4		If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?			X		A.12.3.1 A.8.2.3	Not applicable for SaaS

Control Domain	Question ID	Control Specification	Consensus Assessment Questions	Yes	No	N/A	FedRAMP Low 800-53	ISO 27001:2013	Notes
	BCR-11.5		If using virtual infrastructure, do you provide tenants with a capability to restore a virtual machine to a previous configuration?			X			Not applicable for SaaS
	BCR-11.6		Does your cloud solution include software/provider independent restore and recovery capabilities?	X					ArcGIS Online Cloud infrastructure providers align with ISO 27001 and FedRAMP moderate requirements. Customers can extract datasets in a variety of standard formats that they can restore wherever they desire
	BCR-11.7		Do you test your backup or redundancy mechanisms at least annually?	X					Redundancy mechanisms tested at least annually
Change Control & Configuration Management *New Development / Acquisition*	CCC-01.1	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.	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	X			CA-1 CM-1 PL-1 PL-2 SA-1 SA-3 SA-4	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	ArcGIS Online procedures established for management or acquisition of new application, systems, databases, infrastructure and services is in alignment with FedRAMP Tailored Low requirements.
Change Control & Configuration Management *Outsourced Development*	CCC-02.1	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).	Are policies and procedures for change management, release, and testing adequately communicated to external business partners?	X			SA-4 SA-5 SA-9	A18.2.1 A.15.1.2 A.12.1.4 8.1* (partial) 8.1*	Customers are notified of coming changes in the status.arcgis.com page
	CCC-02.2		Are policies and procedures adequately enforced to ensure external business partners comply with change management requirements?	X					
Change Control & Configuration *Management Quality Testing*	CCC-03.1	Organizations shall follow a defined quality change control and testing process (e.g., ITIL Service Management) with established baselines, testing, and release standards which focus on system availability, confidentiality, and integrity of systems and services.	Do you have a defined quality change control and testing process in place based on system availability, confidentiality, and integrity?	X			CM-1 CM-2 SA-3 SA-4 SA-5	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 A.14.2.3 8.1* partial A.14.2.4 A.12.6.1 A.16.1.3 A.18.2.2 A.18.2.3	ArcGIS Online has a configuration management plan in place.
	CCC-03.2		Is documentation describing known issues with certain products/services available?	X					ArcGIS Online know issues are documented through an internal issues/ticketing system with detailed description of the issue. The Status page and Trust Center announcements provide awareness of any significant current issues.
	CCC-03.3		Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	X					ArcGIS Online has a vulnerability Risk Assessment Process in place as part of the Continuous Monitoring Plan. This process is used to triage each reported security vulnerability or bug before it is submitted to the respective development team in form of a Change Request(CR). Each CR submitted for ArcGIS Online must include a change description, implementation plan, assessed level of risk, impact analysis, back out plan, assigned resources and a test plan prior to being improved. All changes are tested and validated in a test environment prior to being pushed to production. External organizations can report security issues via our Trust Center, report a security concern area, which is managed by our Product Security Incident Response Team (PSIRT).
	CCC-03.4		Do you have controls in place to ensure that standards of quality are being met for all software development?	X					Separate infrastructure utilized for development, staging and production environments allowing validation of quality before deployment to production operations

Control Domain	Question ID	Control Specification	Consensus Assessment Questions	Yes	No	N/A	FedRAMP Low 800-53	ISO 27001:2013	Notes
	CCC-03.5		Do you have controls in place to detect source code security defects for any outsourced software development activities?	X					ArcGIS Online has a vulnerability Risk Assessment Process in place as part of the Continuous Monitoring Plan. This process is used to triage each reported security vulnerability or bug before it is submitted to the respective development team in form of a Change Request(CR). Each CR submitted for ArcGIS Online must include a change description, implementation plan, assessed level of risk, impact analysis, back out plan, assigned resources and a test plan prior to being improved. All changes are tested and validated in a test environment prior to being pushed to production.
	CCC-03.6		Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	X					Flagged as part of periodic code reviews.
Change Control & Configuration Management *Unauthorized Software Installations*	CCC-04.1	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.	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	X			CM-1 CM-2 CM-7 CM-8 SA-6 SA-7 SI-1 SI-3	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	Flagged as part of periodic code reviews.
Change Control & Configuration Management *Production Changes*	CCC-05.1	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.	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?		X		CA-1 CA-6 CA-7 CM-2 CM-6 PL-2 PL-5 SI-2	A.12.1.4 8.1* (partial) A.14.2.2 8.1* (partial) A.14.2.3	The detailed change management procedures and documentation are not distributed. Customers can view update plans based on the status.arcgis.com webpage.
	CCC-05.2		Do you have policies and procedures established for managing risks with respect to change management in production environments?	X					All changes to the ArcGIS Online infrastructure are tracked and recorded through the Change Management documented processes and Procedures, scheduled maintenance windows are published to the ArcGIS Online Status dashboard where any customer can subscribe to for updates at https://status.arcgis.com.
	CCC-05.3		Do you have technical measures in place to ensure that changes in production environments are registered, authorized and in adherence with existing SLAs?	X					ArcGIS Online procedures established for management or acquisition of new application, systems, databases, infrastructure and services is in alignment with FedRAMP Tailored Low requirements.
Data Security & Information Lifecycle Management *Classification*	DSI-01.1	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.	Do you provide a capability to identify data and virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?	X			RA-2	A.8.2.1	ArcGIS Online virtual instances are tagged with unique ID based off the infrastructure provider for better identification. Virtual instances are spun off the same baselined image with appropriate CIS benchmarks applied.
	DSI-01.2		Do you provide a capability to identify data and hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?			X			Hardware is transparent to customer of SaaS offering
Data Security & Information Lifecycle Management	DSI-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to inventory, document, and	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?	X			-	Clause 4.2 5.2, 7.5,	

Control Domain	Question ID	Control Specification	Consensus Assessment Questions	Yes	No	N/A	FedRAMP Low 800-53	ISO 27001:2013	Notes
Data Inventory / Flows	DSI-02.2	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.	Can you ensure that data does not migrate beyond a defined geographical residency?	X				8.1	By default all customer data and metadata is restricted to being stored on US Soil within ArcGIS Online. Starting with the 8.1 release of ArcGIS Online, customers will be able to purchase a new organization and specify storage of their organization data and services into a Asia Pacific region and European Union region offerings. To ensure strong assurance and segmentation, changing data and service location is NOT an option after an organization has been purchased. All customers will continue to utilize the central Portal located on US soil for storing users, access control information, and metadata. All ingress into the ArcGIS Online is encrypted and restricted to port 443. However, the customer can choose to export this data out to any geographical region anytime they please to.
Data Security & Information Lifecycle Management *E-commerce Transactions*	DSI-03.1	Data related to electronic commerce (e-commerce) 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.	Do you provide standardized (e.g. ISO/IEC) non-proprietary encryption algorithms (3DES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	X			AC-1 AC-2 AC-22 AU-1	A.8.2.1 A.13.1.1 A.13.1.2 A.14.1.2 A.14.1.3 A.18.1.4	ArcGIS Online provides encryption at REST with AES-256, and encryption in transit with HTTPS via TLS 1.2.
	DSI-03.2		Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	X					HTTPS with TLS 1.2 utilized
Data Security & Information Lifecycle Management *Handling / Labeling / Security Policy*	DSI-04.1	Policies and procedures shall be established for labeling, handling, and the security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.	Are policies and procedures established for data labeling and handling in order to ensure the security of data and objects that contain data?	X			AC-1 MP-1 PE-1 PE-16 SI-1 SI-12	A.8.2.2 A.8.3.1 A.8.2.3 A.13.2.1	ArcGIS Online customers retain ownership of their data and may implement a labeling and handling policy and procedures to meet their requirements.
	DSI-04.2		Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?	X					ArcGIS Online data labeling is based on the FedRAMP Tailored Low requirements. It is the responsibility of the customer to correctly label and categorize their datasets - Our products support numerous data interoperability standards as described here: https://www.esri.com/en-us/arcgis/open-vision/standards/data-interoperability
	DSI-04.3		Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?		X				ArcGIS Online customers retain ownership of their data and may implement a labeling and handling policy and procedures to meet their requirements.
Data Security & Information Lifecycle Management *Nonproduction Data*	DSI-05.1	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.	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	X			-	A.8.1.3 A.12.1.4 A.14.3.1 8.1* (partial) A.14.2.2.	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. We recommend customers utilize a separate staging organization from the production one for testing purposes. 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.
Data Security & Information Lifecycle Management *Ownership / Stewardship*	DSI-06.1	All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.	Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated?	X			CA-2 CA-2 (1) PS-2 RA-2 SA-2	A.6.1.1 A.8.1.2 A.18.1.4	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.
Data Security & Information Lifecycle	DSI-07.1	Policies and procedures shall be established with supporting business processes and technical measures	Do you support the secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data?	X			MP-6 PE-1	A.11.2.7 A.8.3.2	See cloud infrastructure provider security documentation for secure deletion procedures.

Control Domain	Question ID	Control Specification	Consensus Assessment Questions	Yes	No	N/A	FedRAMP Low 800-53	ISO 27001:2013	Notes
Management *Secure Disposal*	DSI-07.2	implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.	Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?		X				Sanitization procedures not distributed, but in alignment with NIST standards.
Datacenter Security *Asset Management*	DCS-01.1	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.	Do you classify your assets in terms of business criticality, service-level expectations, and operational continuity requirements?	X			-	Annex A.8	
	DCS-01.2		Do you maintain a complete inventory of all of your critical assets located at all sites/ or geographical locations and their assigned ownership?	X					ArcGIS Online inventory listing of all critical assets and ownership is maintained based on the FedRAMP Tailored Low requirements
Datacenter Security *Controlled Access Points*	DCS-02.1	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.	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented for all areas housing sensitive data and information systems?	X			PE-2 PE-3 PE-6 PE-7 PE-8	A.11.1.1 A.11.1.2	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/enus/trustcenter/Compliance Amazon Web Services: https://aws.amazon.com/compliance/
Datacenter Security *Equipment Identification*	DCS-03.1	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.	Do you have a capability to use system geographic location as an authentication factor?	X			IA-4	-	Users are unable to authenticate or utilize ArcGIS Online from U.S. government embargoed countries based on IP address geolocation as identified within Esri's Export Compliance link listed here at: https://www.esri.com/en-us/legal/export-compliance
	DCS-03.2		Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	X					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
Datacenter Security *Offsite Authorization*	DCS-04.1	Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.	Is authorization obtained prior to relocation or transfer of hardware, software, or data to an offsite premises?			X	AC-17 MA-1 PE-1 PE-16	A.11.2.6 A.11.2.7	Not Applicable for SaaS offering
Datacenter Security *Offsite Equipment*	DCS-05.1	Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premise. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full write 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.	Can you provide tenants with your asset management policies and procedures?	X			CM-8	A.8.1.1 A.8.1.2	See cloud infrastructure provider security documentation.
Datacenter Security *Policy*	DCS-06.1	Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in	Can you provide evidence that policies, standards, and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas?	X			PE-2 PE-3 PE-6	A.11.1.1 A.11.1.2	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.

Control Domain	Question ID	Control Specification	Consensus Assessment Questions	Yes	No	N/A	FedRAMP Low 800-53	ISO 27001:2013	Notes
	DCS-06.2	offices, rooms, facilities, and secure areas storing sensitive information.	Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards, and procedures?	X					A certificate of training completion is provided to every employee after the training annually. The third party assessor reviews these materials.
Datacenter Security *Secure Area Authorization*	DCS-07.1	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.	Are physical access control mechanisms (e.g. CCTV cameras, ID cards, checkpoints) in place to secure, constrain and monitor egress and ingress points?	X			PE-7 PE-16	A.11.1.6	Cloud infrastructure provider policies define and establish controls for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information.
Datacenter Security *Unauthorized Persons Entry*	DCS-08.1	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.	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	X			MA-1 MA-2 PE-16	A.11.2.5 8.1* (partial) A.12.1.2	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
Datacenter Security *User Access*	DCS-09.1	Physical access to information assets and functions by users and support personnel shall be restricted.	Do you restrict physical access to information assets and functions by users and support personnel?	X			PE-2 PE-3 PE-6	A.11.1.1	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
Encryption & Key Management *Entitlement*	EKM-01.1	Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.	Do you have key management policies binding keys to identifiable owners?	X			-	Annex A.10.1 A.10.1.1 A.10.1.2	Key management policies, procedures, and processes for ArcGIS Online align with FedRAMP Tailored Low requirements.
Encryption & Key Management *Key Generation*	EKM-02.1	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.	Do you have a capability to allow creation of unique encryption keys per tenant?		X		SC-12 SC-13	Clauses 5.2(c)	Unique keys are utilized per hosted feature service database server, not per database instance.
	EKM-02.2		Do you have a capability to manage encryption keys on behalf of tenants?	X				5.3(a) 5.3(b)	
	EKM-02.3		Do you maintain key management procedures?	X				7.5.3(b) 7.5.3(d)	ArcGIS Online operational keys are managed by the ArcGIS Online Operations Leads. Critical keys are rotated periodically
	EKM-02.4		Do you have documented ownership for each stage of the lifecycle of encryption keys?	X				8.1 8.3	Keys are maintained by the ArcGIS Online Operational Lead
	EKM-02.5		Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	X				9.2(g) A.8.2.3 A.10.1.2 A.18.1.5	Cloud infrastructure provider key management systems utilized
Encryption & Key Management *Encryption*	EKM-03.1	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) and data in	Do you encrypt tenant data at rest (on disk/storage) within your environment?	X			AC-1 AC-18 IA-7 SC-1 SC-7 SC-13	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	Data is encrypted at rest with AES-256 which is a FIPS 140-2 compliant encryption algorithms. This is in alignment with FedRAMP Tailored Low requirements
	EKM-03.2		Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	X					ArcGIS Online utilizes encryption in transit and at-rest by default. 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.

Control Domain	Question ID	Control Specification	Consensus Assessment Questions	Yes	No	N/A	FedRAMP Low 800-53	ISO 27001:2013	Notes
	EKM-03.3	transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.	Do you have documentation establishing and defining your encryption management policies, procedures, and guidelines?	X				A.18.1.4	This documentation is assessed annually as part of the ArcGIS Online FedRAMP authorization
Encryption & Key Management *Storage and Access*	EKM-04.1	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.	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	X			-	Annex A.10.1 A.10.1.1 A.10.1.2	ArcGIS Online implements FIPS 140-2 compliant cryptographic algorithms as a FedRAMP Tailored Low requirement
	EKM-04.2		Are your encryption keys maintained by the cloud consumer or a trusted key management provider?	X					ArcGIS Online encryption keys are maintained by the ArcGIS Online operations team but stored in Cloud Service Provider Key Management Service which is FIP 140-2 compliant and also in alignment with the FedRAMP Tailored Low requirements.
	EKM-04.3		Do you store encryption keys in the cloud?	X					ArcGIS Online encryption keys are maintained by the ArcGIS Online operations team but stored in Cloud Service Provider Key Management Service which is FIP 140-2 compliant and also in alignment with the FedRAMP Tailored Low requirements.
	EKM-04.4		Do you have separate key management and key usage duties?		X				Administrators manage the key management system and consume the keys from it.
Governance and Risk Management *Baseline Requirements*	GRM-01.1	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.	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	X			CM-2 SA-2 SA-4	A.14.1.1 A.18.2.3	ArcGIS Online systems are based off the same baseline with CIS Level 1 benchmarks implemented. The Cloud Infrastructure providers who are ISO 270001 certified manage the backend routers, DNS servers and hypervisors
	GRM-01.2		Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	X					As part of the overall FedRAMP accreditation, baseline security requirements are constantly being reviewed, improved and implemented as part of a Continuous Monitoring Program.
Governance and Risk Management *Risk Assessments*	GRM-02.1	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	Does your organization's risk assessments take into account awareness of data residency, legal and statutory requirements for retention periods and data protection and classification?	X			CA-3 RA-2 RA-3 SI-12	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	
	GRM-02.2		Do you conduct risk assessments associated with data governance requirements at least once a year?	X					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.
Governance and Risk Management *Management Oversight*	GRM-03.1	Managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to their area of responsibility.	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	X			AT-2 AT-3 AT-4 CA-1 CA-5 CA-6 CA-7	Clause 7.2(a,b) A.7.2.1 A.7.2.2 A.9.2.5 A.18.2.2	Managers of ArcGIS Online employees are responsible for ensuring awareness of applicable security policies and procedures for team members.
Governance and Risk Management *Management*	GRM-04.1	An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	X			-	All in sections 4, 5, 6, 7, 8, 9,	An overview of ArcGIS Online security may be found within the ArcGIS Trust Center. Our system security plan information may be shared under NDA.

Control Domain	Question ID	Control Specification	Consensus Assessment Questions	Yes	No	N/A	FedRAMP Low 800-53	ISO 27001:2013	Notes
Program	GRM-04.2	that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and	Do you review your Information Security Management Program (ISMP) at least once a year?	X				10. A.6.1.1 A.13.2.4 A.6.1.3	The ArcGIS Online ISMP is reviewed/audited annually by a 3rd party assessor, artifacts and assessment details are posted in the FedRAMP repository. Cloud infrastructure providers implement ISO 27001 certified ISMP's.
Governance and Risk Management *Management Support / Involvement*	GRM-05.1	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.	Do executive and line management take formal action to support information security through clearly-documented direction and commitment, and ensure the action has been assigned?	X			CM-1	All in section 5 plus clauses 4.4 4.2(b) 6.1.2(a)(1) 6.2 6.2(a) 6.2(d)	Esri's security policies are signed and reviewed by executive management and disseminated to team members in alignment with the FedRAMP accreditation.
Governance and Risk Management *Policy*	GRM-06.1	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.	Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/function and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)?	X			AC-1 AT-1 AU-1 CA-1 CM-1 IA-1 IR-1 MA-1 MP-1 PE-1 PL-1 PS-1 SA-1 SC-1 SI-1	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	Esri's security policies and procedures are in alignment with FedRAMP authorization, GDPR as well as CCPA regulations. Appropriate flow downs are provided to external providers.
	GRM-06.2		Are information security policies 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?	X					Esri has a corporate CISO for oversight of Esri internal operations and product CISO for oversight of ArcGIS.
	GRM-06.3		Do you have agreements to ensure your providers adhere to your information security and privacy policies?	X					
	GRM-06.4		Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or standards?	X					ArcGIS Online undergoes an Annual FedRAMP assessment. A summary of the assessment can be provided upon signing an NDA.
	GRM-06.5		Do you disclose which controls, standards, certifications, and/or regulations you comply with?	X					ArcGIS Online has a FedRAMP Tailored Low ATO and is both GDPR and CCPA aligned
Governance and Risk Management *Policy Enforcement*	GRM-07.1	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.	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	X			PL-4 PS-1 PS-8	A7.2.3	This is documented in the Esri employee handbook which is distributed and signed off upon completion of the new hire training.
	GRM-07.2		Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	X					Prior to accessing ArcGIS Online , all employees must acknowledge and sign a Rules of Behavior (RoB) document that outlines technical and organizational responsibilities related to the access and use of ArcGIS Online , a FedRAMP-Tailored LOW system. Key securities policies are also highlighted in the document. The employees must adhere to the terms of the RoB and the RoB is reviewed/updated/re-signed at least every three years.
Governance and Risk Management *Business / Policy Change Impacts*	GRM-08.1	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.	Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective?	X			AC-1 AT-1 AU-1 CA-1 CM-1 CP-1 IA-1	Clause 4.2.1 a, 4.2(b) 4.3 c, 4.3(a&b) 4.4 5.1(c)	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.
Governance and Risk Management *Policy Reviews*	GRM-09.1	The organization's business leadership (or other accountable business role or function) shall review the information	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	X			AC-1 AT-1 AU-1	Clause 8.1 A.5.1.2	Significant privacy and security announcements are make within the ArcGIS Trust Center announcements which has an RSS feed that may be subscribed to.

Control Domain	Question ID	Control Specification	Consensus Assessment Questions	Yes	No	N/A	FedRAMP Low 800-53	ISO 27001:2013	Notes
	GRM-09.2	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.	Do you perform, at minimum, annual reviews to your privacy and security policies?	X			CA-1 CM-1 CP-1 IA-1 IA-5 IA-5 (1) IR-1 MA-1		As part of the continuous monitoring process, a full security control review and risk assessment is conducted annually which includes associated policies, procedures and standards as they relate to ArcGIS Online . The yearly review is conducted by an accredited third party assessment organization (3rd party assessor). ArcGIS Online IaaS providers undergo the same assessment as part of their FedRAMP authorization maintenance
Governance and Risk Management *Assessments*	GRM-10.1	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).	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	X			CM-1 RA-1 RA-2 RA-3	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) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3)	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.
	GRM-10.2		Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories?	X					
Governance and Risk Management *Program*	GRM-11.1	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.	Do you have a documented, organization-wide program in place to manage risk?	X			AC-1 AT-1 AU-1 CA-1 CA-6 CA-7 PL-1	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)	
	GRM-11.2		Do you make available documentation of your organization-wide risk management program?	X					Every personnel who is read into the ArcGIS Online FedRAMP program has access to risk management plan document.
Human Resources *Asset Returns*	HRS-01.1	Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period.	Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-owned assets?	X			PS-4	A.8.1.1 A.8.1.2 A.8.1.4	Customers have complete ownership of their data at all times. Customer datasets are deleted within 60 days of contract termination unless otherwise specified by the customer.
	HRS-01.2		Do you have asset return procedures outlining how assets should be returned within an established period?			X			There are no assets to be returned to customers. Customer datasets are deleted within 60 days of contract termination unless otherwise specified by the customer.
Human Resources *Background Screening*	HRS-02.1	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.	Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification?	X			PS-2 PS-3	A.7.1.1	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.
Human Resources *Employment Agreements*	HRS-03.1	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.	Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies?	X			PS-1 PS-2 PS-6 PS-7	A.13.2.4 A.7.1.2	ArcGIS Online has a detailed Roles and Responsibilities Matrix as part of the System Security Plan (SSP) with supporting security training materials. Esri employees accessing ArcGIS Online must sign a Rules of Behavior (RoB) that outlines employee technical and organizational responsibilities related to access and use.
	HRS-03.2		Do you require that employment agreements are signed by newly hired or on-boarded workforce personnel prior to granting workforce personnel user access to corporate facilities, resources, and assets?	X					Esri employees accessing ArcGIS Online must sign a Rules of Behavior (RoB) that outlines employee technical and organizational responsibilities related to access and use.
Human Resources *Employment Termination*	HRS-04.1	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.	Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?	X			PS-2 PS-4 PS-5 PS-6 PS-8	A.7.3.1	Esri Human Resources Policy drives employee termination processes for ArcGIS Online. These policies are available to all Esri employees
	HRS-04.2		Do the above procedures and guidelines account for timely revocation of access and return of assets?	X					

Control Domain	Question ID	Control Specification	Consensus Assessment Questions	Yes	No	N/A	FedRAMP Low 800-53	ISO 27001:2013	Notes
Human Resources *Portable / Mobile Devices*	HRS-05.1	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).	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones, and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?	X			AC-17 AC-18 AC-19 MP-2 MP-6	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	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.
Human Resources *Non-Disclosure Agreements*	HRS-06.1	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.	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals?	X			PL-4 PS-6 SA-9	A.13.2.4	Esri Legal Counsel manages and periodically revises the Esri NDA to reflect ArcGIS Online business needs.
Human Resources *Roles / Responsibilities*	HRS-07.1	Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	X			PL-4 PS-1 PS-2 PS-6 PS-7	Clause 5.3 A.6.1.1 A.6.1.1	ArcGIS Online has a Customer Responsibility Matrix which explains and outlines in detail the responsibilities for both the tenants and the service provider to maintain alignment with FedRAMP requirements.
Human Resources *Acceptable Use*	HRS-08.1	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.	Do you have policies and procedures in place to define allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices and IT infrastructure network and systems components?	X			AC-2 AC-8 AC-20 PL-4	A.8.1.3	
	HRS-08.2		Do you define allowance and conditions for BYOD devices and its applications to access corporate resources?	X					Esri has a BYOD policy that is posted internally and mobile security and acceptable use is part of the awareness training program
Human Resources *Training / Awareness*	HRS-09.1	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.	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model, segregation of duties implications, and conflicts of interest) for all persons with access to tenant data?	X			AT-1 AT-2 AT-3 AT-4	Clause 7.2(a), 7.2(b) A.7.2.2	Annual role based & security awareness training is provided for ArcGIS Online employees.
	HRS-09.2		Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	X					When training is completed, a certificate/record of completion or attendance is kept for future reference
	HRS-09.3		Do you document employee acknowledgment of training they have completed?	X					A training certificate is provided as an artifact upon completion of the required training
	HRS-09.4		Is successful and timed completion of the training program(s) considered a prerequisite for acquiring and maintaining access to sensitive systems?	X					Before granting access to systems or resources for ArcGIS Online, employees have to complete certain training modules as a pre-requisite
	HRS-09.5		Are personnel trained and provided with awareness programs at least once a year?	X					ArcGIS Online employees complete security training at least annually.

Control Domain	Question ID	Control Specification	Consensus Assessment Questions	Yes	No	N/A	FedRAMP Low 800-53	ISO 27001:2013	Notes
	HRS-09.6		Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	X					
Human Resources *User Responsibility*	HRS-10.1	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	Are personnel informed of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards, and applicable regulatory requirements?	X			AT-2 AT-3 AT-4 PL-4	Clause 7.2(a), 7.2(b) A.7.2.2 A.9.3.1 A.11.2.8	Annual training for ArcGIS Online is required which includes these aspects.
	HRS-10.2		Are personnel informed of their responsibilities for maintaining a safe and secure working environment?	X					ArcGIS Online employees adhere to a rules of behavior policy outlining user responsibilities. This includes guidance on safeguarding resources used to administer ArcGIS Online
	HRS-10.3		Are personnel informed of their responsibilities for ensuring that equipment is secured and not left unattended?	X					ArcGIS Online employees adhere to a rules of behavior policy outlining user responsibilities. This includes guidance on safeguarding resources used to administer ArcGIS Online
Human Resources *Workspace*	HRS-11.1	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 had been disabled after an established period of inactivity.	Are all computers and laptops configured such that there is lockout screen after a pre-defined amount of time?	X			MP-1 MP-2	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	
	HRS-11.2		Are there policies and procedures to ensure that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents?	X					Policies and procedures enforce limiting access to customer data and if necessary to view as part of a ticketed case the materials are never left unattended.
Identity & Access Management *Audit Tools Access*	IAM-01.1	Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?	X			AU-9	-	All access to the infrastructure is monitored, tracked and recorded through native security services offered by the Cloud Service provider.
	IAM-01.2		Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	X					All access to the infrastructure is monitored, tracked and recorded through native security services offered by the Cloud Service provider.
Identity & Access Management *User Access Policy*	IAM-02.1	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	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	X			AC-1 AC-7 AC-14 IA-1	A.9.1.1 A.9.2.1, A.9.2.2 A.9.2.5 A.9.1.2 A.9.4.1	When an Esri employee assigned to ArcGIS Online transfers to another department or team where s/he does not need to have access to ArcGIS Online anymore, access is revoked as soon as the ArcGIS Online Program Manager is notified and the security team engaged to update status
	IAM-02.2		Do you have policies, procedures and technical measures in place to ensure appropriate data/assets access management in adherence to legal, statutory or regulatory compliance requirements?	X					
	IAM-02.3		Do you have procedures and technical measures in place for user account entitlement de-/provisioning based on the rule of least privilege?	X					ArcGIS Online relies on the Role Based Access Control (RBAC) model. All users in solution need to have a role for which they are granted access to.
	IAM-02.4		Do you have procedures and technical measures in place for data access segmentation in multi-tenant system architectures?	X					Each customer receives their own SQL Azure database for hosted feature services.
	IAM-02.5		Do you enforce data access permissions based on the rules of Authentication, Authorization and Accountability (AAA)?	X					
	IAM-02.6		Do your policies and procedures incorporate security controls for establishing higher levels of assurance for critical business case considerations, supported by multifactor authentication?	X					ArcGIS online system administrators always use Multifactor authenication and customers may enable based on their buisness needs.

Control Domain	Question ID	Control Specification	Consensus Assessment Questions	Yes	No	N/A	FedRAMP Low 800-53	ISO 27001:2013	Notes
	IAM-02.7	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)	Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?		X				
Identity & Access Management *Diagnostic / Configuration Ports Access*	IAM-03.1	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	Is user access to diagnostic and configuration ports restricted to authorized individuals and applications?	X			CM-7 MA-4 MA-5	A.13.1.1 A.9.1.1 A.9.4.4	Only specified users are allowed to access cloud service infrastructure for administrative functions
Identity & Access Management *Policies and Procedures*	IAM-04.1	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	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	X			-	Annex A.9.2 A.9.2.1	
	IAM-04.2		Do you manage and store the user identity of all personnel who have network access, including their level of access?	X				A.9.2.2 A.9.2.3, A.9.2.4, A.9.2.5,	See response in IAM-04.1 above
Identity & Access Management *Segregation of Duties*	IAM-05.1	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.	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	X			AC-1 AC-2 AU-1 AU-2 AU-6	A.6.1.2	ArcGIS Online is a SaaS offering and users do not have administrative access to the backend infrastructure. ArcGIS Online Customers have administration capabilities with in the application only. Customers are responsible for managing their user access to the application by leveraging a SAML 2.0 compliant Identity Provider (IdP). All source code access is restricted to the Esri development team.
Identity & Access Management *Source Code Access Restriction*	IAM-06.1	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	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?	X			-	Clause 5.2(c) 5.3(a), 5.3(b), 7.5.3(b) 7.5.3(d) 8.1, 8.3	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
	IAM-06.2		Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?	X					ArcGIS Online relies on the Role Based Access Control (RBAC) model. All users in solution need to have a role for which they are granted access to
Identity & Access Management *Third Party Access*	IAM-07.1	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.	Does your organization conduct third-party unauthorized access risk assessments?	X			AC-1 AT-1 AU-1 CA-1 CM-1 CP-1 IA-1 IA-5 IA-5 (1) IR-1 MA-1	A.9.2.6 A.9.1.1	Third party assessments are performed annually in alignment with FedRAMP requirements.
	IAM-07.2		Are preventive, detective corrective compensating controls in place to mitigate impacts of unauthorized or inappropriate access?	X				A.9.2.1, A.9.2.2 A.9.2.5	
Identity & Access Management *User Access Restriction / Authorization*	IAM-08.1	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.	Do you document how you grant, approve and enforce access restrictions to tenant/customer credentials following the rules of least privilege?			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,	Customers have the responsibility to grant access to their ArcGIS Online organization. All ArcGIS Online administration personnel must complete the read-in process to the FedRAMP program before they are granted access to any ArcGIS Online resources. No access to customer data is granted.
	IAM-08.2		Based on the rules of least privilege, do you have policies and procedures established for permissible storage and access of identities used for authentication?	X					

Control Domain	Question ID	Control Specification	Consensus Assessment Questions	Yes	No	N/A	FedRAMP Low 800-53	ISO 27001:2013	Notes
	IAM-08.3		Do you limit identities' replication only to users explicitly defined as business necessary?			X		A.9.3.1, A.9.4.1,	Identities are not replicated.
Identity & Access Management *User Access Authorization*	IAM-09.1	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 of the service and/or customer (tenant) has some shared responsibility over implementation of	Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners, and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems, and network components?	X			AC-3 IA-2 IA-2 (1) IA-4 IA-5 IA-5 (1) IA-8 MA-5 PS-6 SA-7	A.9.2.1, A.9.2.2 A.9.2.3 A.9.1.2 A.9.4.1	Customers have the responsibility to grant access to their ArcGIS Online organization. All ArcGIS Online administration personnel must complete the read-in process to the FedRAMP program before they are granted access to any ArcGIS Online resources. No access to customer data is granted.
	IAM-09.2		Do you provide upon the request of users with legitimate interest access (e.g., employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	X					Granting access to customer data is a customer responsibility. Customers can choose to provide other organizations access to their datasets/services. If support asked to provide access, customer is referred to their administrator.
Identity & Access Management *User Access Reviews*	IAM-10.1	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.	Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (exclusive of users maintained by your tenants), based on the rule of least privilege, by business leadership or other accountable business role or function?	X			AC-2 AU-6 PS-6 PS-7	A.9.2.5	ArcGIS Online an annual access re-certification of every user/administrator who has been read into the FedRAMP program and has a role/function in the ArcGIS Online operations.
	IAM-10.2		Do you collect evidence to demonstrate that the policy (see question IAM-10.1) has been enforced?	X					Evidence of this is provided to the 3rd party assessor annually during the annual FedRAMP assessment
	IAM-10.3		Do you ensure that remediation actions for access violations follow user access policies?	X					ArcGIS Online is in alignment with GDPR and CCPA regulations and the requirement for notification of breach is 72 hours. Esri will notify customers about inappropriate access to their data after a confirmation has been made that their data was inappropriately accessed.
	IAM-10.4		Will you share user entitlement and remediation reports with your tenants, if inappropriate access may have been allowed to tenant data?	X					ArcGIS Online is in alignment with GDPR and CCPA regulations and the requirement for notification of breach is 72 hours. Esri will notify customers about inappropriate access to their data after a confirmation has been made that their data was inappropriately accessed.
Identity & Access Management *User Access Revocation*	IAM-11.1	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	Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties?	X			AC-2 PS-4 PS-5	Annex A A.9.2.6 A.9.1.1 A.9.2.1, A.9.2.2 A.9.2.3	Customers are responsible for managing access to the applications and services customers host on ArcGIS Online. The use of Organizational 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. ArcGIS Online system administrator access removed within 1 day of change of status.
	IAM-11.2		Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	X					ArcGIS Online access provisioning includes account creations, permission granting, modifications, updates, and revocations
Identity & Access Management *User ID Credentials*	IAM-12.1	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-	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	X			AC-1 AC-2 AC-3 AU-2 AU-11 IA-1 IA-2	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	Organizations should utilize ArcGIS Online Organizational Logins (SAML 2.0) 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 Organizational Logins may be found at: https://doc.arcgis.com/en/arcgis-online/administer/enterprise-logins.htm

Control Domain	Question ID	Control Specification	Consensus Assessment Questions	Yes	No	N/A	FedRAMP Low 800-53	ISO 27001:2013	Notes
	IAM-12.2	service application (API) and information processing interoperability (e.g., SSO and Federation)	Do you use open standards to delegate authentication capabilities to your tenants?	X			IA-2 (1) IA-5 IA-5 (1) IA-6 IA-8		Customers are responsible for managing authentication & access to their the ArcGIS Online application using a SAML 2.0 compliant Identity Provider (IdP)
	IAM-12.3	• Account credential lifecycle management from instantiation through revocation	Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	X					(IdP). IAM-12.3 Do you support identity federation standards (e.g., SAML, SPML, WS- Federation, etc.) as a means of authenticating/authorizing users? Yes A
	IAM-12.4	• Account credential and/or identity store minimization or re-use when feasible	Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?		X				
	IAM-12.5	• Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)	Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?		X				Data Classification is a customer responsibility. However, ArcGIS Online has a FedRAMP Tailored Low ATO. This can be used by the customers as a baseline for classifying what type of data they should be hosting in the solution
	IAM-12.6		Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access?	X					ArcGIS Online has the option to enable Multifactor Authentication(MFA). For details please review the resource below: https://doc.arcgis.com/en/arcgis-online/administer/configure-security.htm
	IAM-12.7		Do you allow tenants to use third-party identity assurance services?	X					
	IAM-12.8		Do you support password (e.g., minimum length, age, history, complexity) and account lockout (e.g., lockout threshold, lockout duration) policy enforcement?	X					This is a Customer Responsibility to enforce the minimum password requirements that meet their agency's security policies.
	IAM-12.9		Do you allow tenants/customers to define password and account lockout policies for their accounts?	X					
	IAM-12.10		Do you support the ability to force password changes upon first logon?	X					
	IAM-12.11		Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?		X				Esri recommendation is to use Organizational Logins (SAML) to facilitate and align with the organization's security requirements. ArcGIS Online accounts gradually unlock after a set period of time.
Identity & Access Management *Utility Programs Access*	IAM-13.1	Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.	Are access to utility programs used to manage virtualized partitions (e.g. shutdown, clone, etc) appropriately restricted and monitored?	X			CM-7	A.9.1.2 A.9.4.4	Less than 20 ArcGIS Online Administrators are responsible for managing ArcGIS instances or images and connect using X.509 certificates. Customers do not have direct access to the cloud infrastrucre systems.
Infrastructure & Virtualization Security *Audit Logging / Intrusion Detection*	IVS-01.1	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.	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?	X			AU-1 AU-2 AU-3 AU-4 AU-5 AU-6 AU-9 AU-11 AU-12 PE-2 PE-3	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	ArcGIS Online implements an Incident Response plan and associated incident detection tools which are in alignment with the FedRAMP Tailored Low requirement.
	IVS-01.2		Is physical and logical user access to audit logs restricted to authorized personnel?	X					Only accessible by the ArcGIS Online infrastructure administrators(Less than 5 people
	IVS-01.3		Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been performed?	X					This information is documented in the ArcGIS Online System Security Plan and this can be obtained with an NDA in place.
	IVS-01.4		Are audit logs centrally stored and retained?	X					Audit logs are retained as defined by ArcGIS online retention policy which is in alignment with FedRAMP Tailored Low requirements.
	IVS-01.5		Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	X					Audit logs are reviewed weekly within the ArcGIS Online solution by the Security team
Infrastructure & Virtualization Security *Change Detection*	IVS-02.1	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	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)?	X			-	Annex A.12.1.2 A.12.4,	ArcGIS Online operations have full logging of all actions and activities in the solution
	IVS-02.2		Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?	X				A.12.4.1, A.12.4.2, A.12.4.3, A.12.6.1, A.12.6.2,	ArcGIS Online security infrastructure exists on an isolated private network subnet. All logs from every instance are stored in a common repository. Implementation ensures only ArcGIS Online Administrators can read logs. Collected logs are not modified or deleted by anyone.

Control Domain	Question ID	Control Specification	Consensus Assessment Questions	Yes	No	N/A	FedRAMP Low 800-53	ISO 27001:2013	Notes
	IVS-02.3	integrity must be immediately available to customers through electronic methods (e.g., portals or alerts).	Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g., portals or alerts)?			X		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	All changes to the ArcGIS Online infrastructure are tracked and recorded through the Change Management documented processes and Procedures, scheduled maintenance windows are published to the ArcGIS Online Status dashboard where any customer can subscribe to for updates at https://status.arcgis.com. Details about virtual machines is not posted as ArcGIS Online is a multitenant SaaS offering.
Infrastructure & Virtualization Security *Clock Synchronization*	IVS-03.1	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.	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	X			AU-1 AU-8	A.12.4.1 A.12.4.4	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.
Infrastructure & Virtualization Security *Capacity / Resource Planning*	IVS-04.1	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.	Do you provide documentation regarding what levels of system (e.g., network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?	X			SA-4	A.12.1.3	ArcGIS Online utilizes the capacity of two major cloud infrastructure providers to meet customer demands and Service Level Agreements (SLA) for availability, quality and capacity. Each cloud provider offers SLAs for their infrastructure
	IVS-04.2		Do you restrict use of the memory oversubscription capabilities present in the hypervisor?			X			ArcGIS Online is a SaaS offering. Hypervisor management is a responsibility of the Cloud Infrastructure Provider AWS or Microsoft Azure.
	IVS-04.3		Does your system's capacity requirements take into account current, projected, and anticipated capacity needs for all systems used to provide services to the tenants?	X					ArcGIS Online as a SaaS offering relies on Cloud Infrastructure technology which give it the ability to auto-scale as needed to cater to the customers needs at any given time.
	IVS-04.4		Is system performance monitored and tuned in order to continuously meet regulatory, contractual, and business requirements for all the systems used to provide services to the tenants?	X					ArcGIS Online Cloud infrastructure is configured for auto scaling in order to provide services that meets customer SLAs
Infrastructure & Virtualization Security *Management - Vulnerability Management*	IVS-05.1	Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g., virtualization aware).	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?	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)	Cloud infrastructure providers virtualization technologies are regularly evaluated internally and by independent assessments annually.
Infrastructure & Virtualization Security *Network Security*	IVS-06.1	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 compensating controls.	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?			X	CM-7 SC-7 SC-20 (1)	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	ArcGIS Online is a SaaS offering to the customers
	IVS-06.2		Do you regularly update network architecture diagrams that include data flows between security domains/zones?	X					All ArcGIS Online architectural diagrams (Networks and systems combined) are reviewed in accordance to the FedRAMP Tailored Low requirements.
	IVS-06.3		Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?	X					ArcGIS Online Access review is done at least once a week as an alignment requirement for FedRAMP Tailored Low ATO
	IVS-06.4		Are all firewall access control lists documented with business justification?	X					This is part of the ArcGIS System Security Plan. Access to the details in the ArcGIS Online SSP can be provided upon signing an NDA
Infrastructure & Virtualization Security *OS Hardening and Base Controls*	IVS-07.1	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.	Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?	X			-	Annex A.12.1.4 A.12.2.1 A.12.4.1 A.12.6.1	ArcGIS Online has developed a system configuration baseline in alignment with industry best practices such as CIS benchmarks and DISA STIGS. Robust network hardening is present within ArcGIS Online . Anti-virus, logging capabilities are ensured and monitored on all systems within ArcGIS Online .

Control Domain	Question ID	Control Specification	Consensus Assessment Questions	Yes	No	N/A	FedRAMP Low 800-53	ISO 27001:2013	Notes
Infrastructure & Virtualization Security *Production / Non-Production Environments*	IVS-08.1	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.	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	X			-	A.12.1.4 A.14.2.9 A.9.1.1	ArcGIS Online utilizes separate production and non-production environments. Customers can purchase a separate non-production organization for testing/staging purposes.
	IVS-08.2		For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?			X		8.1,partial, A.14.2.2	ArcGIS Online is not an IaaS
	IVS-08.3		Do you logically and physically segregate production and non-production environments?		X			8.1,partial, A.14.2.3 8.1,partial, A.14.2.4	ArcGIS Online utilizes logically separate production and non-production environments (environment is not physically separate).
Infrastructure & Virtualization Security *Segmentation*	IVS-09.1	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	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	X			SC-7	A.13.1.3 A.9.4.1 A.18.1.4	Cloud infrastructure provider network segmentation aligns with ISO 27001 standards. Cloud infrastructure provider firewalls are utilized to separate various ArcGIS Online components.
	IVS-09.2		Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legal, regulatory and contractual requirements?	X					Cloud infrastructure provider network segmentation aligns with ISO 27001 standards. Cloud infrastructure provider firewalls are utilized to separate various ArcGIS Online components.
	IVS-09.3		Have you implemented the necessary measures for the appropriate isolation and segmentation of tenants' access to infrastructure system and network components, in adherence to established policies, legal, statutory, and regulatory compliance obligations?	X					Cloud infrastructure provider network segmentation aligns with ISO 27001 standards. Cloud infrastructure provider firewalls are utilized to separate various ArcGIS Online components.
	IVS-09.4		Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	X					ArcGIS Online security infrastructure exists on an isolated private network subnet. All logs from every instance are stored in a common repository. Implementation ensures only ArcGIS Online Administrators can read logs. Collected logs are not modified or deleted by anyone.
	IVS-09.5		Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	X					See response in IVS-09.1 above
Infrastructure & Virtualization Security *VM Security - Data Protection*	IVS-10.1	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.	Are secured and encrypted communication channels used when migrating physical servers, applications, or data to virtual servers?	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)	Customers can migrate data to ArcGIS Online using HTTPS via TLS 1.2 only for encrypted communication. Customers can also deploy a separate non-production ArcGIS Online organization for initial data migrating /testing efforts.
	IVS-10.2		Do you use a network segregated from production-level networks when migrating physical servers, applications, or data to virtual servers?			X			ArcGIS Online is a SaaS offering not an IaaS offering
Infrastructure & Virtualization Security *VMM Security - Hypervisor Hardening*	IVS-11.1	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).	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	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)	This is managed by the cloud infrastructure service providers, see there security documentation for details.
Infrastructure & Virtualization Security *Wireless Security*	IVS-12.1	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,	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?	X			AC-1 AC-18 CM-6 SC-7	A.8.1.1 A.8.1.2 A.8.1.3 A.11.2.1 A.11.2.4 A.13.1.1	Protection of wireless devices and ensuring encryption are part of regular network management security practices within Esri which includes monitoring. Wireless is not utilized as part of the cloud infrastructure provider environments. Access from a wireless network on a customer premise to the ArcGIS Online environment must be secured by the customer
	IVS-12.2		Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, SNMP community strings)?	X				A.13.1.2 A.13.2.1 A.8.3.3 A.12.4.1 A.9.2.1,	See response in IVS-12.1 above

Control Domain	Question ID	Control Specification	Consensus Assessment Questions	Yes	No	N/A	FedRAMP Low 800-53	ISO 27001:2013	Notes
	IVS-12.3	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	Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?	X				A.9.2.2 A.13.1.3 A.10.1.1 A.10.1.2	See response in IVS-12.1 above
Infrastructure & Virtualization Security *Network Architecture*	IVS-13.1	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.	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?	X			CM-7 SC-7 SC-20 (1)	A.13.1.1 A.13.1.2 A.14.1.2	See ArcGIS Online security presentation materials within the ArcGIS Trust Center documents.
	IVS-13.2		Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?	X				A.12.4.1 A.9.1.2 A.13.1.3 A.18.1.4	ArcGIS Online utilizes AWS & Microsoft Azure native FedRAMP authorized security features to route users to ArcGIS Online resources, these Cloud Service Provider features provide protection against attacks such as common DDoS attack.
Interoperability & Portability *APIs*	IPY-01.1	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?		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)	Main API's for ArcGIS Online customers are summarized within the documentation. Not all API's are listed. https://doc.arcgis.com/en/arcgis-online/reference/develop-with-agol.htm
Interoperability & Portability *Data Request*	IPY-02.1	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).	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	X			-	Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2),	Customers retain ownership of their data at all times and can export their data from ArcGIS Online in standard formats at any time. ArcGIS Online item types are described here: https://doc.arcgis.com/en/arcgis-online/reference/supported-items.htm
Interoperability & Portability *Policy & Legal*	IPY-03.1	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.	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?	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)	The ArcGIS Online REST API is publicly available See IPY-01.1 Legal aspects are addressed as part of the Terms of Service at: http://www.esri.com/legal/pdfs/mla_e204_e300/english#Addendum_3 See the ArcGIS Online SLA within the ArcGIS Trust Center documents.
	IPY-03.2		If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?			X			Not Applicable for SaaS
	IPY-03.3		Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?	X					https://www.esri.com/content/dam/esrisites/en-us/media/legal/referenced-files/g- 632-ArcGIS Online l-service-level.pdf
Interoperability & Portability *Standardized Network Protocols*	IPY-04.1	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.	Is data import, data export, and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	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)	ArcGIS Online data in transit is over HTTPS via TLS 1.2 Only.
	IPY-04.2		Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	X					See the ArcGIS Online Trust Center for details. ArcGIS Online only utilizes HTTPS via port 443 and TLS 1.2 for current organizations.
Interoperability & Portability *Virtualization*	IPY-05.1	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	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?		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)	We utilize cloud provider native images for ideal performance as the user does not interact with the underlying infrastructure of ArcGIS Online directly.
	IPY-05.2		If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?			X			Not Applicable for SaaS

Control Domain	Question ID	Control Specification	Consensus Assessment Questions	Yes	No	N/A	FedRAMP Low 800-53	ISO 27001:2013	Notes
	IPY-05.3	customer review.	Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?	X				6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2)	See the cloud infrastructure provider documentation for hypervisor information.
Mobile Security *Anti-Malware*	MOS-01.1	Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?			X	-	Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2),	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
Mobile Security *Application Stores*	MOS-02.1	A documented list of approved application stores has been communicated as acceptable for mobile devices accessing or storing provider managed data.	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?			X	-	Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2),	See response in MOS-01.1 above
Mobile Security *Approved Applications*	MOS-03.1	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.	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto a mobile device?			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)	See response in MOS-01.1 above
Mobile Security *Approved Software for BYOD*	MOS-04.1	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.	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?	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)	Esri has a BYOD policy that is posted internally and mobile security and acceptable use is part of the awareness training program
Mobile Security *Awareness and Training*	MOS-05.1	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.	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?	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)	This mobile usage training is part of the new hire on-boarding process which every employee is part of.
Mobile Security *Cloud Based Services*	MOS-06.1	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.	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?			X	-	Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2),	See response in MOS-01.1 above
Mobile Security *Compatibility*	MOS-07.1	The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.	Do you have a documented application validation process for testing device, operating system, and application compatibility issues?			X	-	Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2),	See response in MOS-01.1 above
Mobile Security *Device Eligibility*	MOS-08.1	The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?	X			-	Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1)	Mobile acceptable usage training is part of the new hire on-boarding process which every employee is part of.

Control Domain	Question ID	Control Specification	Consensus Assessment Questions	Yes	No	N/A	FedRAMP Low 800-53	ISO 27001:2013	Notes
Mobile Security *Device Inventory*	MOS-09.1	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.	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (e.g., operating system and patch levels, lost or decommissioned, device assignee)?			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)	See response in MOS-01.1 above
Mobile Security *Device Management*	MOS-10.1	A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?			X	-	Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2),	See response in MOS-01.1 above
Mobile Security *Encryption*	MOS-11.1	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.	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?	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)	Encryption is enforced on the ArcGIS Administration devices
Mobile Security *Jailbreaking and Rooting*	MOS-12.1	The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting) and is enforced through detective and preventative controls on the device or through a centralized device management system (e.g., mobile device management).	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?			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),	See response in MOS-01.1 above
	MOS-12.2		Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?			X			See response in MOS-01.1 above
Mobile Security *Legal*	MOS-13.1	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 over the loss of non-company data in the case that a wipe of the device is required.	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery, and legal holds?	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)	
	MOS-13.2		Does the BYOD policy clearly state the expectations over the loss of non-company data in case a wipe of the device is required?	X					
Mobile Security *Lockout Screen*	MOS-14.1	BYOD and/or company owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?			X	-	Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2),	See response in MOS-01.1 above
Mobile Security *Operating Systems*	MOS-15.1	Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.	Do you manage all changes to mobile device operating systems, patch levels, and applications via your company's change management processes?			X	-	Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2),	See response in MOS-01.1 above
Mobile Security *Passwords*	MOS-16.1	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.	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?			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)	See response in MOS-01.1 above
	MOS-16.2		Are your password policies enforced through technical controls (i.e. MDM)?			X			See response in MOS-01.1 above
	MOS-16.3		Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?			X			See response in MOS-01.1 above

Control Domain	Question ID	Control Specification	Consensus Assessment Questions	Yes	No	N/A	FedRAMP Low 800-53	ISO 27001:2013	Notes
Mobile Security *Policy*	MOS-17.1	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).	Do you have a policy that requires BYOD users to perform backups of specified corporate data?			X	-	Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2),	See response in MOS-01.1 above
	MOS-17.2		Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?			X			See response in MOS-01.1 above
	MOS-17.3		Do you have a policy that requires BYOD users to use anti-malware software (where supported)?			X			See response in MOS-01.1 above
Mobile Security *Remote Wipe*	MOS-18.1	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	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?			X	-	Clause 6.1.1, 6.1.1(e)(2) 6.1.2	See response in MOS-10.1
	MOS-18.2		Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?			X			See response in MOS-10.1
Mobile Security *Security Patches*	MOS-19.1	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	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?			X	-	Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2),	See response in MOS-10.1
	MOS-19.2		Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?			X			See response in MOS-10.1
Mobile Security *Users*	MOS-20.1	The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?			X	-	3) 9.3(d) 9.3(e) 9.3(f)	See response in MOS-01.1 above
	MOS-20.2		Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?			X			See response in MOS-01.1 above
Security Incident Management, E-Discovery, & Cloud Forensics *Contact / Authority Maintenance*	SEF-01.1	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.	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	X			-	A.6.1.3 A.6.1.4	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.
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Management*	SEF-02.1	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.	Do you have a documented security incident response plan?	X			IR-1 IR-2 IR-4 IR-5 IR-6 IR-7	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	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.
	SEF-02.2		Do you integrate customized tenant requirements into your security incident response plans?		X				Customers may specify a primary incident contact as part of their contract.
	SEF-02.3		Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	X					Responsibilities are delineated within the ArcGIS Online Customer Responsibility Matrix(CRM).
	SEF-02.4		Have you tested your security incident response plans in the last year?	X					Incident response plan tested annually
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Reporting*	SEF-03.1	Workforce personnel and external business relationships shall be informed of their responsibility 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.	Are workforce personnel and external business relationships adequately informed of their responsibility, and, if required, consent and/or contractually required to report all information security events in a timely manner?	X			IR-2 IR-6 IR-7 SI-5	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)	
	SEF-03.2		Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations?	X					All incidents are reported through Esri PSIRT
Security Incident Management, E-Discovery, & Cloud	SEF-04.1	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	X			AU-6 AU-9 AU-11	Clause 5.2 (c), 5.3 (a),	ArcGIS Online Incident Response plan is in alignment with the FedRAMP Tailored Low requirements.

Control Domain	Question ID	Control Specification	Consensus Assessment Questions	Yes	No	N/A	FedRAMP Low 800-53	ISO 27001:2013	Notes
Forensics *Incident Response Legal Preparation*	SEF-04.2	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.	Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	X			IR-5 IR-7 IR-8	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),	
	SEF-04.3		Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	X					Customer organization administrator can disable user access or contact our support team to temporarily disable the organization.
	SEF-04.4		Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	X					See response in SEF-04.3 above
Security Incident Management, E-Discovery, & Cloud Forensics	SEF-05.1	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	X			IR-4 IR-5 IR-8	A.16.1.6	Information security incidents are classified into severity levels and processed according to the severity level.
	SEF-05.2		Will you share statistical information for security incident data with your tenants upon request?		X				This is considered company confidential data
Supply Chain Management, Transparency, and Accountability *Data Quality and Integrity*	STA-01.1	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.	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?	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)	
	STA-01.2		Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	X					ArcGIS Online uses cloud infrastructure providers whose risk management practices align with ISO 27001 and FedRAMP Moderate requirements.
Supply Chain Management, Transparency, and Accountability *Incident Reporting*	STA-02.1	The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals).	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?	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)	General site information for ArcGIS Online is available via the Status page of the Trust.ArcGIS.com website. If a security incident were to affect numerous customers it would be announced via the ArcGIS Trust Center. Information about customer specific incidents can be viewed via the MyEsri Support portal.
Supply Chain Management, Transparency, and Accountability *Network / Infrastructure Services*	STA-03.1	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.	Do you collect capacity and use data for all relevant components of your cloud service offering?	X			CA-3 SA-9	A.15.1.2 A.13.1.2	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/enus/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.
	STA-03.2		Do you provide tenants with capacity planning and use reports?	X					Capacity is unlimited and therefore not reported, however within the status page of an ArcGIS Online or the administrator can see credits consumed, content and app usage.
Supply Chain Management, Transparency, and Accountability *Provider Internal Assessments*	STA-04.1	The provider shall perform annual internal assessments of conformance and effectiveness of its policies, procedures, and supporting measures and metrics.	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	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)	As part of FedRAMP Tailored Low compliance, ArcGIS Online implements a robust continuous monitoring program to monitor risk which includes internal assessments at least annually.
Supply Chain Management, Transparency, and Accountability *Third Party Agreements*	STA-05.1	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	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted?	X			CA-3 PS-7 SA-6 SA-7 SA-9	A.15.1.2, 8.1* partial, A.13.2.2, A.9.4.1 A.10.1.1	Third party agreements are reviewed by Esri Contracts and/or Legal Counsel as appropriate.
	STA-05.2		Do you select and monitor outsourced providers to ensure that they are in compliance with applicable legislation?	X					Third party agreements are reviewed by Esri Contracts and/or Legal Counsel as appropriate. And ArcGIS Online related service providers are validated at least annually in alignment with FedRAMP.
	STA-05.3		Does legal counsel review all third-party agreements?	X					See response in STA-05.1 above
	STA-05.4		Do third-party agreements include provision for the security and protection of information and assets?	X					

Control Domain	Question ID	Control Specification	Consensus Assessment Questions	Yes	No	N/A	FedRAMP Low 800-53	ISO 27001:2013	Notes
	STA-05.5	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 development and information exchange, usage, and integrity persistence	Do you have the capability to recover data for a specific customer in the case of a failure or data loss?		X				Customers have full responsibility to backup and restore their datasets.
	STA-05.6		Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	X					By default all customer data and metadata is restricted to being stored on US Soil within ArcGIS Online. Starting with the 8.1 release of ArcGIS Online, customers will be able to purchase a new organization and specify storage of their organization data and services into a Asia Pacific and European Union region offerings. To ensure strong assurance and segmentation, changing data and service location is NOT an option after an organization has been purchased. All customers will continue to utilize the central Portal located on US soil for storing users, access control information, and metadata.
	STA-05.7		Can you provide the physical location/geography of storage of a tenant's data upon request?	X					By default 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). Starting with the 8.1 release of ArcGIS Online, customers will be able to purchase a new organization and specify storage of their organization data and services into a new European Union (EU1) region offering. Customers utilizing the EU1 region will store their data within Amazon Web Service regions EU-West-1 (Ireland) with failover to EU-Central-1 (Germany) and Microsoft Azure regions North Europe (Ireland) with failover to West Europe (Netherlands). AWS Primary: ap-southeast-2 (Sydney) AWS Failover: ap-southeast-1 (Singapore), Azure Primary: Australia East; Azure Failover: Australia Southeast.
	STA-05.8		Can you provide the physical location/geography of storage of a tenant's data in advance?	X					By default 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). Starting with the 8.1 release of ArcGIS Online, customers will be able to purchase a new organization and specify storage of their organization data and services into a new European Union (EU1) region offering. Customers utilizing the EU1 region will store their data within Amazon Web Service regions EU-West-1 (Ireland) with failover to EU-Central-1 (Germany) and Microsoft Azure regions North Europe (Ireland) with failover to West Europe (Netherlands). AWS Primary: ap-southeast-2 (Sydney) AWS Failover: ap-southeast-1 (Singapore), Azure Primary: Australia East; Azure Failover: Australia Southeast.
	STA-05.9		Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?	X					By default 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). Starting with the 8.1 release of ArcGIS Online, customers will be able to purchase a new organization and specify storage of their organization data and services into a new European Union (EU1) region offering. Customers utilizing the EU1 region will store their data within Amazon Web Service regions EU-West-1 (Ireland) with failover to EU-Central-1 (Germany) and Microsoft Azure regions North Europe (Ireland) with failover to West Europe (Netherlands). AWS Primary: ap-southeast-2 (Sydney) AWS Failover: ap-southeast-1 (Singapore), Azure Primary: Australia East; Azure Failover: Australia Southeast.
	STA-05.10		Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	X					Esri's privacy policy is in alignment GDPR as well as CCPA regulations. Customers are notified within 72 hours if their data is confirmed breached

Control Domain	Question ID	Control Specification	Consensus Assessment Questions	Yes	No	N/A	FedRAMP Low 800-53	ISO 27001:2013	Notes
	STA-05.11		Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?	X					EU-based org need to opt-in to enable access and other customers can opt-out of the Esri User Experience Improvement Program for ArcGIS Online. https://support.esri.com/en/technical-article/000016235
	STA-05.12		Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?	X					ArcGIS Online subprocessors are delineated within the ArcGIS Online Data Processing Addendum (DPA)
Supply Chain Management, Transparency, and Accountability *Supply Chain Governance Reviews*	STA-06.1	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.	Do you review the risk management and governance processes of partners to account for risks inherited from other members of that partner's supply chain?	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 *Supply Chain Metrics*	STA-07.1	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 non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate, and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	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) 8.1 8.3	See response in STA-03.1 above
	STA-07.2		Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?		X				Continuously improving coverage
	STA-07.3		Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	X					
	STA-07.4		Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	X					See ArcGIS Trust Center - https://status.arcgis.com
	STA-07.5		Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	X					ArcGIS Online standards are based on FedRAMP Tailored Low requirements. Also, this Cloud Security Alliance (CSA) CAIQ for ArcGIS Online is available to customers.
	STA-07.6		Do you provide customers with ongoing visibility and reporting of your SLA performance?	X					See ArcGIS Trust Center - https://status.arcgis.com
	STA-07.7		Do your data management policies and procedures address tenant and service level conflicts of interests?	X					
	STA-07.8		Do you review all service level agreements at least annually?	X					
Supply Chain Management, Transparency, and Accountability *Third Party Assessment*	STA-08.1	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.	Do you assure reasonable information security across your information supply chain by performing an annual review?	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)	ArcGIS Online uses cloud infrastructure providers whose information security & risk management practices align with stringent ISO 27001 and FedRAMP Moderate requirements. Esri reviews the providers at least annually
	STA-08.2		Does your annual review include all partners/third-party providers upon which your information supply chain depends?	X					See response in STA-08.1 for more information
Supply Chain Management, Transparency, and Accountability *Third Party Audits*	STA-09.1	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.	Do you mandate annual information security reviews and audits of your third party providers to ensure that all agreed upon security requirements are met?	X			AC-1 AT-1 AU-1 CA-1 CM-1 CP-1 IA-1 IA-7 IR-1 MA-1 MP-1	A.15.1.2 8.1* partial, 8.1* partial, A.15.2.1 A.13.1.2	Minimum baseline checked annually and additional auditng performed ad-hoc.
	STA-09.2		Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	X					Performed external ad-hoc as necessary
Threat and Vulnerability Management	TVM-01.1	Policies and procedures shall be established, and supporting business processes and technical measures	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your IT infrastructure network and systems components?	X			SC-5 SI-3 SI-5	A.12.2.1	All systems in ArcGIS Online as well as administrator workstations have anti-malware installed. This is in alignment to FedRAMP Tailored Low requirements.

Control Domain	Question ID	Control Specification	Consensus Assessment Questions	Yes	No	N/A	FedRAMP Low 800-53	ISO 27001:2013	Notes
Antivirus / Malicious Software	TVM-01.2	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.	Do you ensure that security threat detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components as prescribed by industry best practices?	X					In alignment with FedRAMP Tailored Low requirements threat detection signatures and behavioral analysis tools used or installed on systems in ArcGIS Online are updated frequently
Threat and Vulnerability Management *Vulnerability / Patch Management*	TVM-02.1	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.	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	X			CM-4 RA-5 SI-1 SI-2 SI-5	8.1*partial, A.14.2.2, 8.1*partial, A.14.2.3 A.12.6.1	Vulnerability assessments against ArcGIS Online are conducted at least monthly as part of the Continuous Monitoring Plan - including system, web application and database scans.
	TVM-02.2		Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	X					See response in TVM-02.1
	TVM-02.3		Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	X					See response in TVM-02.1
	TVM-02.4		Will you make the results of vulnerability scans available to tenants at their request?	X					Customers can request a copy of the most recent Continuous Monitoring (ConMon) Report under NDA to see how vulnerabilities are addressed on a continuous basis
	TVM-02.5		Do you have a capability to patch vulnerabilities across all of your computing devices, applications, and systems?	X					ArcGIS Online releases which include patches and bug fixes are performed quarterly. Security patched are deployed monthly by default, however critical risk vulnerabilities are patched within 7 days
	TVM-02.6		Do you inform customers (tenant) of policies and procedures and identified weaknesses if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control?	X					Customer best practice is provided via the ArcGIS Trust Center and Security Advisor Tool.
Threat and Vulnerability Management *Mobile Code*	TVM-03.1	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.	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?			X	-	A.12.2.1	ArcGIS Online does not require installable mobile code such as MS ActiveX, Adobe Flash, and MS Silverlight.
	TVM-03.2		Is all unauthorized mobile code prevented from executing?			X			See response in TVM-03.1 above