ArcGIS Online
Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire (CAIQ) 4.0.2 June 2023

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 261 questions a cloud consumer and cloud auditor may wish to ask of a cloud provider.

The CSA is a "not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing" (https://cloudsecurityalliance.org/about/). A wide range of industry security practitioners, corporations, and associations participate in this organization to achieve its mission. Esri has been ArcGIS Online CSA answers since 2013, with the most recent update being make for the latest CAIQ 4.0.2 questionnaire.

ArcGIS Online is audited annually by a 3rd party assessor to ensure alignment with its Federal Risk and Authorization Management Program (FedRAMP) 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 customer 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

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control Title	CCM Domain Title
A&A-01.1	Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	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 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.	Audit and Assurance Policy and Procedures	Audit & Assurance
A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually?	Yes	CSP-owned	Audit and assurance polices, procedure and standards are established, documented and approved annually.		
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?	Yes	CSP-owned	ArcGIS Online solution is annually assessed/audited by an independent 3rd party assessor as per FedRAMP requirements which utilizes NIST standards.	Independent Assessments	
A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies?	Yes	CSP-owned	ArcGIS Online solution is annually assessed/audited by a 3rd party assessor as per FedRAMP requirements which is based on a risk management framework.	Risk Based Planning Assessment	
A&A-04.1	Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit?	Yes	CSP-owned	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. Along with OWASP Top 10 and SANS 25 ArcGIS Online is FedRAMP authorized and therefore 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.	Requirements Compliance	
A&A-05.1	Is an audit management process defined and implemented to support audit planning, risk analysis, security control assessments, conclusions, remediation schedules, report generation, and reviews of past reports and supporting evidence?	Yes	CSP-owned	ArcGIS Online solution is annually assessed/audited by a 3rd party assessor as per FedRAMP requirements.	Audit Management Process	
A&A-06.1	Is a risk-based corrective action plan to remediate audit findings established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	ArcGIS Online has a Risk Assessment Process in place as part of the Continuous Monitoring Plan, with includes the generation of a Plan of Actions and Milestones (POAM) for resolution.	Remediation	
A&A-06.2	Is the remediation status of audit findings reviewed and reported to relevant stakeholders?	Yes	CSP-owned	Esri will notify customers about inappropriate access to their data after a confirmation has been made that their data was inappropriately accessed. Web, system and database scans as part of FedRAMP requirements are reviewed and reported. Static, 3rd party analysis is removed and reported https://trust.arcgis.com/en/ for Security Announcements are published to serve as notification of security information		
AIS-01.1	Are application security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to guide appropriate planning, delivery, and support of the organization's application security capabilities?	Yes	CSP-owned	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 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	Application and Interface Security Policy and Procedures	
AIS-01.2	Are application security policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	As part of the implemented FedRAMP program Security polices and procedures along with security related areas associated with FedRAMP NIST 800-53 controls are reviewed and updated at least annually.		
AIS-02.1	Are baseline requirements to secure different applications established, documented, and maintained?	Yes	CSP-owned	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	Application Security Baseline Requirements	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control Title	CCM Domain Title
AIS-03.1	Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?	Yes	CSP-owned	As part of FedRAMP compliance, ArcGIS Online implements a robust continuous monitoring program to monitor risk which includes monthly metric review and internal assessments at least annually. Dashboards are also used for performance review and analysis.	Application Security Metrics	Application & Interface Security
AIS-04.1	Is an SDLC process defined and implemented for application design, development, deployment, and operation per organizationally designed security requirements?	Yes	CSP-owned	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 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.	Secure Application Design and Development	
AIS-05.1	Does the testing strategy outline criteria to accept new information systems, upgrades, and new versions while ensuring application security, compliance adherence, and organizational speed of delivery goals?	Yes	CSP-owned	ArcGIS Online performs a significant impact assessment for new information systems, upgrades and maintenance. The changes are assessed by the Development and Security Teams to understand operational and security impact. Results are presented to the Configuration Management Board for final decision determination.	Automated Application Security Testing	
AIS-05.2	Is testing automated when applicable and possible?	Yes	CSP-owned	Development Teams perform automated unit tests and end to end testing. Security performs dynamic scans that must be remediated before moving to production		
AIS-06.1	Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?	Yes	CSP-owned	Nearly all code is covered in automated testing through our secure development lifecycle prior to release	Automated Secure Application Deployment	
AIS-06.2	Is the deployment and integration of application code automated where possible?	Yes	CSP-owned	Deployments when triggered are automated to ensure that baselines are pulled from code repos and to ensure that modifications are not made directly to the production area		
AIS-07.1	Are application security vulnerabilities remediated following defined processes?	Yes	CSP-owned	Security vulnerabilities are prioritized based on risk assessment. Teams are expected to remediate or provide mitigation based on risk level	Application Vulnerability Remediation	
AIS-07.2	Is the remediation of application security vulnerabilities automated when possible?	Yes	CSP-owned	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).		
BCR-01.1	Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	ArcGIS Online has a full Continuity Plan designed in alignment with FedRAMP requirements. The plan has been tested.	Business Continuity Management Policy and Procedures	
BCR-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	ArcGIS Online has a full Continuity Plan designed in alignment with FedRAMP requirements. The plan has been tested. This is assessed by a 3rd party to ensure compliance.		
BCR-02.1	Are criteria for developing business continuity and operational resiliency strategies and capabilities established based on business disruption and risk impacts?	Yes	Shared CSP and 3rd-party	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.	Risk Assessment and Impact Analysis	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control Title	CCM Domain Title
BCR-03.1	Are strategies developed to reduce the impact of, withstand, and recover from business disruptions in accordance with risk appetite?	Yes	CSP-owned	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.	Business Continuity Strategy	Business Continuity Management and Operational Resilience
BCR-04.1	Are operational resilience strategies and capability results incorporated to establish, document, approve, communicate, apply, evaluate, and maintain a business continuity plan?	Yes	CSP-owned	ArcGIS Online maintains a contingency plan and incident response plan that is in alignment with FedRAMP requirements. Documents are reviewed by external auditors as part of FedRAMP requirements.	Business Continuity Planning	
BCR-05.1	Is relevant documentation developed, identified, and acquired to support business continuity and operational resilience plans?	Yes	CSP-owned	ArcGIS Online has a full Continuity Plan designed in alignment with FedRAMP-requirements.	Documentation	
BCR-05.2	Is business continuity and operational resilience documentation available to authorized stakeholders?	Yes	CSP-owned	ArcGIS Online Business Continuity plan is not shared publicly however, all relevant internal stakeholders have access to the plan.		
BCR-05.3	Is business continuity and operational resilience documentation reviewed periodically?	Yes	CSP-owned	Esri's Business continuity plan is reviewed periodically.		
BCR-06.1	Are the business continuity and operational resilience plans exercised and tested at least annually and when significant changes occur?	Yes	CSP-owned	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 Exercises	
BCR-07.1	Do business continuity and resilience procedures establish communication with stakeholders and participants?	Yes	CSP-owned	Every personnel who is read into the ArcGIS Online FedRAMP program has access to risk management plan document.	Communication	
BCR-08.1	Is cloud data periodically backed up?	Yes	Shared CSP and CSC	Customers have full responsibility to backup and restore their datasets. Esri is responsible for backup of the infrastructure.	Backup	
BCR-08.2	Is the confidentiality, integrity, and availability of backup data ensured?	Yes	Shared CSP and CSC	Esri does backup infrastructure data and customer is responsible for backup of their data at whatever frequency they desire. Data is encrypted at rest with AES-256 which is a FIPS 140-2 compliant encryption algorithms. This is in alignment with FedRAMP requirements		
BCR-08.3	Can backups be restored appropriately for resiliency?	Yes	CSP-owned	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-09.1	Is a disaster response plan established, documented, approved, applied, evaluated, and maintained to ensure recovery from natural and man-made disasters?	Yes	CSP-owned	ArcGIS Online has a full Continuity Plan designed in alignment with FedRAMP security control requirements. ArcGIS Online cloud Infrastructure providers ensure their business continuity plans align with ISO 27001 standards.	Disaster Response Plan	
BCR-09.2	Is the disaster response plan updated at least annually, and when significant changes occur?	Yes	CSP-owned	The plan is reviewed and tested annually together as part of our continuity plan.		
BCR-10.1	Is the disaster response plan exercised annually or when significant changes occur?	Yes	CSP-owned	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.	Response Plan Exercise	
BCR-10.2	Are local emergency authorities included, if possible, in the exercise?	No	CSP-owned	Local emergency authorities are not included in annual testing.		

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control Title	CCM Domain Title
BCR-11.1	Is business-critical equipment supplemented with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards?	Yes	Shared CSP and 3rd-party	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	Equipment Redundancy	
CCC-01.1	Are risk management policies and procedures associated with changing organizational assets including applications, systems, infrastructure, configuration, etc., established, documented, approved, communicated, applied, evaluated and maintained (regardless of whether asset management is internal or external)?	Yes	CSP-owned	Teams perform impact assessments based on functionality, security and privacy. This would cover both application and infrastructure changes to ArcGIS Online.	Change Management Policy and Procedures	Change Control and Configuration Management
CCC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	The configuration management plan and associated procedures are reviewed and updated at least annually. Our configuration management plan highlights security impact assessments to understand risk when handing both application and infrastructure. Changes are flow though Dev, QA then to PROD. During this time Teams are testing and evaluating risk impact.		
CCC-02.1	Is a defined quality change control, approval and testing process (with established baselines, testing, and release standards) followed?	Yes	CSP-owned	ArcGIS Online procedures established for management or acquisition of new application, systems, databases, infrastructure and services is in alignment with FedRAMP requirements.	Quality Testing	
CCC-03.1	Are risks associated with changing organizational assets (including applications, systems, infrastructure, configuration, etc.) managed, regardless of whether asset management occurs internally or externally (i.e., outsourced)?	Yes	CSP-owned	Changes to our baselines are CM managed regardless of whether asset management occurs internally or externally.	Change Management Technology	
CCC-04.1	Is the unauthorized addition, removal, update, and management of organization assets restricted?	Yes	Shared CSP and 3rd-party	Development and DevOPs Teams have access to update application code/ configuration and infrastructure configuration through CM procedures. Only authorized Team members have direct access to AWS and Azure. This is reviewed at least quarterly.	Unauthorized Change Protection	
CCC-05.1	Are provisions to limit changes that directly impact CSC-owned environments and require tenants to authorize requests explicitly included within the service level agreements (SLAs) between CSPs and CSCs?	NA	CSP-owned	Hardware is transparent to customer of SaaS offering. No customer equipment resides in the SaaS offering	Change Agreements	
CCC-06.1	Are change management baselines established for all relevant authorized changes on organizational assets?	Yes	CSP-owned	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.	Change Management Baseline	
CCC-07.1	Are detection measures implemented with proactive notification if changes deviate from established baselines?	Yes	CSP-owned	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.	Detection of Baseline Deviation	
CCC-08.1	Is a procedure implemented to manage exceptions, including emergencies, in the change and configuration process?	Yes	CSP-owned	This is part of the Configuration Management plan	Exception	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control Title	CCM Domain Title
CCC-08.2	Is the procedure aligned with the requirements of the GRC-04: Policy Exception Process?'	Yes	CSP-owned	This is part of the Configuration Management plan and in alignment with FedRAMP requirements	Management	
CCC-09.1	Is a process to proactively roll back changes to a previously known "good state" defined and implemented in case of errors or security concerns?	Yes	CSP-owned	The CM process includes reverting baselines to known stable state if there is a deployment issue.	Change Restoration	
CEK-01.1	Are cryptography, encryption, and key management policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Key management policies, procedures, and processes for ArcGIS Online align with FedRAMP requirements.	Encryption and Key Management Policy and Procedures	
CEK-01.2	Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Key management policies and procedures are reviewed and updated annually.		
CEK-02.1	Are cryptography, encryption, and key management roles and responsibilities defined and implemented?	Yes	CSP-owned	ArcGIS Online operational keys are managed by the ArcGIS Online Operations Leads. Critical keys are rotated periodically	CEK Roles and Responsibilities	
CEK-03.1	Are data at-rest and in-transit cryptographically protected using cryptographic libraries certified to approved standards?	Yes	CSP-owned	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.	Data Encryption	
CEK-04.1	Are appropriate data protection encryption algorithms used that consider data classification, associated risks, and encryption technology usability?	Yes	CSP-owned	ArcGIS Online provides encryption at REST with AES-256, and encryption in transit with HTTPS via TLS 1.2.	Encryption Algorithm	
CEK-05.1	Are standard change management procedures established to review, approve, implement and communicate cryptography, encryption, and key management technology changes that accommodate internal and external sources?	Yes	CSP-owned	See CEK-01.1	Encryption Change Management	
CEK-06.1	Are changes to cryptography-, encryption- and key management-related systems, policies, and procedures, managed and adopted in a manner that fully accounts for downstream effects of proposed changes, including residual risk, cost, and benefits analysis?	Yes	CSP-owned	Key management policies, procedures, and processes for ArcGIS Online align with FedRAMP requirements. Endpoints are validated against SSL Labs and evolving standards regularly reviewed.	Encryption Change Cost Benefit Analysis	
CEK-07.1	Is a cryptography, encryption, and key management risk program established and maintained that includes risk assessment, risk treatment, risk context, monitoring, and feedback provisions?	Yes	CSP-owned	ArcGIS Online has established an information security management program with designated roles and responsibilities that are appropriately aligned within the organization. Esri management reviews and evaluates the risks identified in the risk management program at least annually. Key management policies, procedures, and processes for ArcGIS Online align with FedRAMP requirements.	Encryption Risk Management	
CEK-08.1	Are CSPs providing CSCs with the capacity to manage their own data encryption keys?	No	Shared CSP and CSC	ArcGIS Online encryption keys are maintained by the ArcGIS Online operations team but stored in Cloud Service Provider Key Management Service which is FIPS 140-2 compliant and also in alignment with FedRAMP requirements. Customers can implement a CASB to encrypt any fields they wan to manage the encryption keys for.	CSC Key Management Capability	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control Title	CCM Domain Title
CEK-09.1	Are encryption and key management systems, policies, and processes audited with a frequency proportional to the system's risk exposure, and after any security event?	Yes	CSP-owned	This documentation is assessed annually as part of the ArcGIS Online FedRAMP authorization	Encryption and Key Management Audit	Cryptography, Encryption & Key Management
CEK-09.2	Are encryption and key management systems, policies, and processes audited (preferably continuously but at least annually)?	Yes	CSP-owned	Key management policies, procedures, and processes for ArcGIS are reviewed annually.		
CEK-10.1	Are cryptographic keys generated using industry-accepted and approved cryptographic libraries that specify algorithm strength and random number generator specifications?	Yes	Shared CSP and 3rd-party	ArcGIS Online encryption keys are maintained by the ArcGIS Online operations team and stored in Cloud Service Provider Key Management Services which are NIST approved and FIPS 140-2 compliant which is in alignment with FedRAMP requirements.	Key Generation	
CEK-11.1	Are private keys provisioned for a unique purpose managed, and is cryptography secret?	Yes	Shared CSP and 3rd-party	ArcGIS Online encryption keys are maintained by the ArcGIS Online operations team and stored in Cloud Service Provider Key Management Services which are NIST approved and FIPS 140-2 compliant which is in alignment with FedRAMP requirements.	Key Purpose	
CEK-12.1	Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements?	Yes	CSP-owned	Critical keys are rotated periodically	Key Rotation	
CEK-13.1	Are cryptographic keys revoked and removed before the end of the established cryptoperiod (when a key is compromised, or an entity is no longer part of the organization) per defined, implemented, and evaluated processes, procedures, and technical measures to include legal and regulatory requirement provisions?	Yes	CSP-owned	Critical keys are rotated in alignment with FedRAMP Moderate requirements. Cryptographic keys are invalidated when compromised or at the end of their defined lifecycle period.	Key Revocation	
CEK-14.1	Are processes, procedures and technical measures to destroy unneeded keys defined, implemented and evaluated to address key destruction outside secure environments, revocation of keys stored in hardware security modules (HSMs), and include applicable legal and regulatory requirement provisions?	Yes	Shared CSP and 3rd-party	ArcGIS Online encryption keys are maintained by the ArcGIS Online operations team and stored in Cloud Service Provider Key Management Services which are NIST approved and FIPS 140-2 compliant which is in alignment with FedRAMP requirements.	Key Destruction	
CEK-15.1	Are processes, procedures, and technical measures to create keys in a pre-activated state (i.e., when they have been generated but not authorized for use) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	NA	Shared CSP and 3rd-party	Keys are managed through KMS and Azure vault. Automatic rotation is in place so a pre-activations state is not utilized.	Key Activation	
CEK-16.1	Are processes, procedures, and technical measures to monitor, review and approve key transitions (e.g., from any state to/from suspension) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	Shared CSP and 3rd-party	Keys are managed through KMS and Azure vault. Automatic rotation is in place	Key Suspension	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control Title	CCM Domain Title
CEK-17.1	Are processes, procedures, and technical measures to deactivate keys (at the time of their expiration date) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	Shared CSP and 3rd-party	Keys are managed through KMS and Azure vault. Automatic rotation is in place	Key Deactivation	
CEK-18.1	Are processes, procedures, and technical measures to manage archived keys in a secure repository (requiring least privilege access) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	Shared CSP and 3rd-party	Keys are managed through KMS and Azure vault. Automatic rotation is in place	Key Archival	
CEK-19.1	Are processes, procedures, and technical measures to encrypt information in specific scenarios (e.g., only in controlled circumstances and thereafter only for data decryption and never for encryption) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	Shared CSP and 3rd-party	ArcGIS Online encryption keys are maintained by the ArcGIS Online operations team and stored in Cloud Service Provider Key Management Services which are NIST approved and FIPS 140-2 compliant which is in alignment with FedRAMP requirements. Customer datasets are always encrypted at rest and in-transit.	Key Compromise	
CEK-20.1	Are processes, procedures, and technical measures to assess operational continuity risks (versus the risk of losing control of keying material and exposing protected data) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	Shared CSP and 3rd-party	ArcGIS Online encryption keys are maintained by the ArcGIS Online operations team and stored in Cloud Service Provider Key Management Services which are NIST approved and FIPS 140-2 compliant which is in alignment with FedRAMP requirements.	Key Recovery	
CEK-21.1	Are key management system processes, procedures, and technical measures being defined, implemented, and evaluated to track and report all cryptographic materials and status changes that include legal and regulatory requirements provisions?	Yes	Shared CSP and 3rd-party	ArcGIS Online encryption keys are maintained by the ArcGIS Online operations team and stored in Cloud Service Provider Key Management Services which are NIST approved and FIPS 140-2 compliant which is in alignment with FedRAMP requirements.	Key Inventory Management	
DCS-01.1	Are policies and procedures for the secure disposal of equipment used outside the organization's premises established, documented, approved, communicated, enforced, and maintained?	Yes	CSP-owned	Sanitization is in alignment with NIST standards	Off-Site Equipment Disposal Policy and Procedures	
DCS-01.2	Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed?	Yes	Shared CSP and 3rd-party	When a storage device has reached the end of its useful life, AWS and MS Azure procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. Both providers use the techniques detailed in NIST 800-88 (“Guidelines for Media Sanitization”) as part of the decommissioning process.		
DCS-01.3	Are policies and procedures for the secure disposal of equipment used outside the organization's premises reviewed and updated at least annually?	Yes	Shared CSP and 3rd-party	AWS and Azure Policies are reviewed approved by the cloud service provider's leadership at least annually or as needed basis.		
DCS-02.1	Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location established, documented, approved, communicated, implemented, enforced, maintained?	NA	CSP-owned	Hardware is transparent to customer of SaaS offering. No customer equipment resides in the SaaS offering	Off-Site Transfer	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control Title	CCM Domain Title
DCS-02.2	Does a relocation or transfer request require written or cryptographically verifiable authorization?	NA	CSP-owned	Not applicable for a SaaS offering	Transfer Authorization Policy and Procedures	Datacenter Security
DCS-02.3	Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location reviewed and updated at least annually?	NA	CSP-owned	Not applicable for a SaaS offering		
DCS-03.1	Are policies and procedures for maintaining a safe and secure working environment (in offices, rooms, and facilities) established, documented, approved, communicated, enforced, and maintained?	Yes	CSP-owned	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.	Secure Area Policy and Procedures	
DCS-03.2	Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms) reviewed and updated at least annually?	Yes	CSP-owned	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.		
DCS-04.1	Are policies and procedures for the secure transportation of physical media established, documented, approved, communicated, enforced, evaluated, and maintained?	NA	CSP-owned	Not Applicable for SaaS offering	Secure Media Transportation Policy and Procedures	
DCS-04.2	Are policies and procedures for the secure transportation of physical media reviewed and updated at least annually?	NA	CSP-owned	Not Applicable for SaaS offering		
DCS-05.1	Is the classification and documentation of physical and logical assets based on the organizational business risk?	Yes	Shared CSP and 3rd-party	ArcGIS Online is operated with FedRAMP Moderate controls based on customer organizational business risk requirements requested of Esri. MS Azure and AWS provide the physical assets for ArcGIS Online and obtain at least the same level of assuarance or higher for thier operations.	Assets Classification	
DCS-06.1	Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system?	Yes	CSP-owned	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	Assets Cataloguing and Tracking	
DCS-07.1	Are physical security perimeters implemented to safeguard personnel, data, and information systems?	Yes	CSP-owned	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.	Controlled Access Points	
DCS-07.2	Are physical security perimeters established between administrative and business areas, data storage, and processing facilities?	Yes	CSP-owned	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.		
DCS-08.1	Is equipment identification used as a method for connection authentication?	Yes	CSP-owned	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	Equipment Identification	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control Title	CCM Domain Title
DCS-09.1	Are solely authorized personnel able to access secure areas, with all ingress and egress areas restricted, documented, and monitored by physical access control mechanisms?	Yes	CSP-owned	Cloud infrastructure provider physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access datacenter floors. No subcontractor access beyond cloud providers	Secure Area Authorization	
DCS-09.2	Are access control records retained periodically, as deemed appropriate by the organization?	Yes	CSP-owned	Cloud infrastructure provider physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access datacenter floors. No subcontractor access beyond cloud providers		
DCS-10.1	Are external perimeter datacenter surveillance systems and surveillance systems at all ingress and egress points implemented, maintained, and operated?	Yes	Shared CSP and 3rd-party	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	Surveillance System	
DCS-11.1	Are datacenter personnel trained to respond to unauthorized access or egress attempts?	Yes	Shared CSP and 3rd-party	See MS Azure and Amazon Web Services security documentation for details	Unauthorized Access Response Training	
DCS-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure risk-based protection of power and telecommunication cables from interception, interference, or damage threats at all facilities, offices, and rooms?	Yes	CSP-owned	ArcGIS Online Business Impact Assessment and updated annually in alignment with FedRAMP standards.. 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.	Cabling Security	
DCS-13.1	Are data center environmental control systems designed to monitor, maintain, and test that on-site temperature and humidity conditions fall within accepted industry standards effectively implemented and maintained?	Yes	CSP-owned	ArcGIS Online is FedRAMP authorized and therefore also aligns with NIST standards.	Environmental Systems	
DCS-14.1	Are utility services secured, monitored, maintained, and tested at planned intervals for continual effectiveness?	Yes	CSP-owned	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.	Secure Utilities	
DCS-15.1	Is business-critical equipment segregated from locations subject to a high probability of environmental risk events?	Yes	Shared CSP and 3rd-party	ArcGIS Online uses geographically redundant datacenter locations across MS Azure and AWS cloud service providers. The AWS Security Operations Center performs quarterly threat and vulnerability reviews of datacenters and colocation sites. These AWS reviews are in addition to an initial environmental and geographic assessment of a site performed prior to building or leasing. The AWS quarterly reviews are validated by third parties during their SOC, PCI, and ISO assessments. Microsoft data center site selection is performed using a number of criteria, including mitigation of environmental risks. For Azure, in areas where the exists a higher probability of earthquakes, seismic bracing of the facility is employed. Data centers are built as redundant, highly-available components of the Azure platform.	Equipment Location	
DSP-01.1	Are policies and procedures established, documented, approved, communicated, enforced, evaluated, and maintained for the classification, protection, and handling of data throughout its lifecycle according to all applicable laws and regulations, standards, and risk level?	Yes	CSP-owned	Details to data handling and protection policies and procedures can be found on our Trust Center: https://trust.arcgis.com/en/	Security and Privacy Policy and Procedures	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control Title	CCM Domain Title
DSP-01.2	Are data security and privacy policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Data and privacy policies and procedures reviewed annually.		
DSP-02.1	Are industry-accepted methods applied for secure data disposal from storage media so information is not recoverable by any forensic means?	Yes	CSP-owned	Sanitization procedures are in alignment with NIST standards.	Secure Disposal	
DSP-03.1	Is a data inventory created and maintained for sensitive and personal information (at a minimum)?	Yes	CSP-owned	Customers determine and manage the types of sensitive and personal data they process based on how they use ArcGIS Online. Because the customer would be the data controller, they are required to create and maintain inventories of the sensitive and personal data they process using ArcGIS Online (this is required by contract).	Data Inventory	
DSP-04.1	Is data classified according to type and sensitivity levels?	Yes	CSP-owned	Data Classification is a customer responsibility. However, ArcGIS Online has a FedRAMP ATO. This can be used by the customers as a baseline for classifying what type of data they should be hosting in the solution.	Data Classification	
DSP-05.1	Is data flow documentation created to identify what data is processed and where it is stored and transmitted?	Yes	CSP-owned	Generalized ArcGIS Online data flow documentation for customers is located in the ArcGIS Trust Center documents found here: https://downloads.esri.com/resources/enterprisegis/ArcGIS_Online_Security.pdf . More detailed operational data flow diagrams are included in the ArcGIS Online System Security Plan and updated at least annually.	Data Flow Documentation	
DSP-05.2	Is data flow documentation reviewed at defined intervals, at least annually, and after any change?	Yes	CSP-owned	Generalized ArcGIS Online data flow documentation for customers is located in the ArcGIS Trust Center documents found here: https://downloads.esri.com/resources/enterprisegis/ArcGIS_Online_Security.pdf . More detailed operational data flow diagrams are included in the ArcGIS Online System Security Plan and updated at least annually.		
DSP-06.1	Is the ownership and stewardship of all relevant personal and sensitive data documented?	Yes	CSP-owned	Customers retain full ownership of their data at all times.	Data Ownership and Stewardship	
DSP-06.2	Is data ownership and stewardship documentation reviewed at least annually?	No	CSC-owned	Customers retain full ownership of their data at all times.		
DSP-07.1	Are systems, products, and business practices based on security principles by design and per industry best practices?	Yes	CSP-owned	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 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.	Data Protection by Design and Default	
DSP-08.1	Are systems, products, and business practices based on privacy principles by design and according to industry best practices?	Yes	CSP-owned	Esri's aligns its privacy practices with industry-recognized privacy principles to implement appropriate administrative, technical and physical controls. Esri aligns privacy engineering decisions with the organization's overall privacy strategy and industry-recognized leading practices of privacy by design and by default.	Data Privacy by Design and Default	
DSP-08.2	Are systems' privacy settings configured by default and according to all applicable laws and regulations?	Yes	CSP-owned	Esri's security and privacy policies and procedures are in alignment with FedRAMP authorization, GDPR as well as CCPA regulations. Appropriate flow downs are provided to external providers.		

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control Title	CCM Domain Title
DSP-09.1	Is a data protection impact assessment (DPIA) conducted when processing personal data and evaluating the origin, nature, particularity, and severity of risks according to any applicable laws, regulations and industry best practices?	NA	CSC-owned	The customer is responsible for conducting a DPIA as GDPR requires controllers to carry out a DPIA where a processing activity is using new technologies and is likely to result in a "high risk to the rights and freedoms" of individuals (Article 35.1 GDPR). Esri is a processor under the articles of GDPR. Customers are expected to analyze the data set that they upload. Esri minimizes data collected by our product.	Data Protection Impact Assessment	Data Security and Privacy Lifecycle Management
DSP-10.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope (as permitted by respective laws and regulations)?	Yes	CSP-owned	Processes, procedures, and technical measures can be found in our Data Processing Addendum: https://www.esri.com/content/dam/esrisites/en-us/media/legal/gdpr-data-processing-addendums/data-process-addend.pdf	Sensitive Data Transfer	
DSP-11.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable data subjects to request access to, modify, or delete personal data (per applicable laws and regulations)?	Yes	CSP-owned	Upon request Esri will provide you with information about whether we hold any of your personal information. Esri will permit you to access, correct, or delete your information in our database by contacting Esri or by logging in to your account and making the appropriate changes. We will respond to all requests for access within a reasonable timeframe.	Personal Data Access, Reversal, Rectification and Deletion	
DSP-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure personal data is processed (per applicable laws and regulations and for the purposes declared to the data subject)?	Yes	CSP-owned	Processes, procedures, and technical measures can be found in our Data Processing Addendum: https://www.esri.com/content/dam/esrisites/en-us/media/legal/gdpr-data-processing-addendums/data-process-addend.pdf	Limitation of Purpose in Personal Data Processing	
DSP-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for the transfer and sub-processing of personal data within the service supply chain (according to any applicable laws and regulations)?	Yes	CSP-owned	Processes, procedures, and technical measures can be found in our Data Processing Addendum: https://www.esri.com/content/dam/esrisites/en-us/media/legal/gdpr-data-processing-addendums/data-process-addend.pdf	Personal Data Sub-processing	
DSP-14.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to disclose details to the data owner of any personal or sensitive data access by sub-processors before processing initiation?	Yes	CSP-owned	Processes, procedures, and technical measures can be found in our Data Processing Addendum: https://www.esri.com/content/dam/esrisites/en-us/media/legal/gdpr-data-processing-addendums/data-process-addend.pdf	Disclosure of Data Sub-processors	
DSP-15.1	Is authorization from data owners obtained, and the associated risk managed, before replicating or using production data in non-production environments?	Yes	CSP-owned	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 as needed to provide the services, or as required by law or regulation or by order of a court or other government body in alignment with our privacy supplement statement.	Limitation of Production Data Use	
DSP-16.1	Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations?	Yes	CSP-owned	Esri has a set ArcGIS Online Data Retention and Disposal Policy that outline Esri's approach to managing the retention and secure disposal of information in line with our business requirements and legal obligations.	Data Retention and Deletion	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control Title	CCM Domain Title
DSP-17.1	Are processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle?	Yes	CSP-owned	Processes, procedures, and technical measures can be found in our Data Processing Addendum: https://www.esri.com/content/dam/esrisites/en-us/media/legal/gdpr-data-processing-addendums/data-process-addend.pdf	Sensitive Data Protection	
DSP-18.1	Does the CSP have in place, and describe to CSCs, the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations?	Yes	CSP-owned	Esri will promptly notify the data exporter about any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to reserve the confidentiality of a law enforcement investigation. Further details can be found in Esri's Data Processing Addendum: https://www.esri.com/content/dam/esrisites/en-us/media/legal/gdpr-data-processing-addendums/data-process-addend.pdf	Disclosure Notification	
DSP-18.2	Does the CSP give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation?	Yes	CSP-owned	Esri will promptly notify the data exporter about any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to reserve the confidentiality of a law enforcement investigation. Further details can be found in Esri's Data Processing Addendum: https://www.esri.com/content/dam/esrisites/en-us/media/legal/gdpr-data-processing-addendums/data-process-addend.pdf		
DSP-19.1	Are processes, procedures, and technical measures defined and implemented to specify and document physical data locations, including locales where data is processed or backed up?	Yes	CSP-owned	By default, all ArcGIS Online customer data resides on United States soil within the confines of the Amazon Web Services US Regions (East, West), and Microsoft Azure US Regions (South Central, East, West). When purchasing a new organization, customers can specify a different region for their data storage. The two alternative regional data hosting locations are the European Union (EU1) and Asia Pacific (AP1) regional offerings. EU1 customer data is stored in Amazon Web Services region EU-West-1 (Ireland) with failover to EU-Central-1 (Germany), and Microsoft Azure region North Europe (Ireland) with failover to West Europe (Netherlands). AP1 customer data is stored in Amazon Web Services region AP-SouthEast-2 (Sydney) with failover to AP-SouthEast-1 (Singapore), and Microsoft Azure region Australia East with failover to Australia SouthEast. Customers are responsible for the backup of their datasets.	Data Location	
GRC-01.1	Are information governance program policies and procedures sponsored by organizational leadership established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Esri's security policies are signed and reviewed by executive management and disseminated to team members in alignment with the FedRAMP accreditation.	Governance Program Policy and Procedures	Governance, Risk and
GRC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Esri's security polices and procedures are reviewed and updated annually		
GRC-02.1	Is there an established formal, documented, and leadership-sponsored enterprise risk management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks?	Yes	CSP-owned	This is part of our FedRAMP program based off NIST 800-53 controls and is audited annually. Esri's security policies and procedures are in alignment with FedRAMP authorization, GDPR as well as CCPA regulations.	Risk Management Program	
GRC-03.1	Are all relevant organizational policies and associated procedures reviewed at least annually, or when a substantial organizational change occurs?	Yes	CSP-owned	As part of the overall FedRAMP accreditation, baseline security requirements are constantly being reviewed, improved and implemented as part of a Continuous Monitoring Program.	Organizational Policy Reviews	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control Title	CCM Domain Title
GRC-04.1	Is an approved exception process mandated by the governance program established and followed whenever a deviation from an established policy occurs?	Yes	CSP-owned	This is part of the Configuration Management plan and followed whenever a deviation from policy occurs.	Policy Exception Process	Compliance
GRC-05.1	Has an information security program (including programs of all relevant CCM domains) been developed and implemented?	Yes	CSP-owned	ArcGIS Online is FedRAMP authorized and the program is based off NIST 800-53 controls	Information Security Program	
GRC-06.1	Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented?	Yes	CSP-owned	ArcGIS Online system administrator roles and responsibilities are documented within the ArcGIS Online System Security Plan. User roles and responsibilities are documented within the ArcGIS Online application documentation.	Governance Responsibility Model	
GRC-07.1	Are all relevant standards, regulations, legal/contractual, and statutory requirements applicable to your organization identified and documented?	Yes	CSP-owned	This documentation is assessed annually as part of the ArcGIS Online FedRAMP authorization	Information System Regulatory Mapping	
GRC-08.1	Is contact established and maintained with cloud-related special interest groups and other relevant entities?	Yes	CSP-owned	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.	Special Interest Groups	
HRS-01.1	Are background verification policies and procedures of all new employees (including but not limited to remote employees, contractors, and third parties) established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	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.	Background Screening Policy and Procedures	
HRS-01.2	Are background verification policies and procedures designed according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, business requirements, and acceptable risk?	Yes	CSP-owned	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.		
HRS-01.3	Are background verification policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Esri corporate policies and procedures are reviewed and updated at least annually.		
HRS-02.1	Are policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	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.	Acceptable Use of Technology Policy and Procedures	
HRS-02.2	Are the policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets reviewed and updated at least annually?	Yes	CSP-owned	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-03.1	Are policies and procedures requiring unattended workspaces to conceal confidential data established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	ArcGIS Online employees adhere to a rules of behavior policy outlining user responsibilities. This includes guidance on safeguarding resources used to administer ArcGIS Online	Clean Desk Policy and	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control Title	CCM Domain Title
HRS-03.2	Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually?	Yes	CSP-owned	ArcGIS Online employees adhere to a rules of behavior policy outlining user responsibilities and review their responsibilities annually.	Procedures	Human Resources
HRS-04.1	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations established, documented, approved, communicated, applied, evaluated, and maintained?	NA	CSP-owned	Esri does not store or process information within remote sites and locations.	Remote and Home Working Policy and Procedures	
HRS-04.2	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations reviewed and updated at least annually?	NA	CSP-owned	Esri does not store or process information within remote sites and locations.		
HRS-05.1	Are return procedures of organizationally-owned assets by terminated employees established and documented?	Yes	CSP-owned	Esri Human Resources Policy drives employee termination processes for ArcGIS Online. These policies are available to all Esri employees	Asset returns	
HRS-06.1	Are procedures outlining the roles and responsibilities concerning changes in employment established, documented, and communicated to all personnel?	Yes	CSP-owned	Esri Human Resources Policy drives employee termination processes for ArcGIS Online. These policies are available to all Esri employees	Employment Termination	
HRS-07.1	Are employees required to sign an employment agreement before gaining access to organizational information systems, resources, and assets?	Yes	CSP-owned	Esri employees accessing ArcGIS Online must sign a Rules of Behavior (RoB) that outlines employee technical and organizational responsibilities related to access and use.	Employment Agreement Process	
HRS-08.1	Are provisions and/or terms for adherence to established information governance and security policies included within employment agreements?	Yes	CSP-owned	Esri employees accessing ArcGIS Online must sign a Rules of Behavior (RoB) that outlines employee technical and organizational responsibilities related to access and use.	Employment Agreement Content	
HRS-09.1	Are employee roles and responsibilities relating to information assets and security documented and communicated?	Yes	CSP-owned	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.	Personnel Roles and Responsibilities	
HRS-10.1	Are requirements for non-disclosure/confidentiality agreements reflecting organizational data protection needs and operational details identified, documented, and reviewed at planned intervals?	Yes	CSP-owned	Esri Legal Counsel manages and periodically revises the Esri NDA to reflect ArcGIS Online business needs.	Non-Disclosure Agreements	
HRS-11.1	Is a security awareness training program for all employees of the organization established, documented, approved, communicated, applied, evaluated and maintained?	Yes	CSP-owned	ArcGIS Online employees complete security training at least annually	Security Awareness Training	
HRS-11.2	Are regular security awareness training updates provided?	Yes	CSP-owned	Annual role based & security awareness training is provided for ArcGIS Online employees.		
HRS-12.1	Are all employees granted access to sensitive organizational and personal data provided with appropriate security awareness training?	Yes	CSP-owned	Annual role based & security awareness training is provided for ArcGIS Online employees.	Personal and Sensitive Data	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control Title	CCM Domain Title
HRS-12.2	Are all employees granted access to sensitive organizational and personal data provided with regular updates in procedures, processes, and policies relating to their professional function?	Yes	CSP-owned	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.	Sensitive Data Awareness and Training	
HRS-13.1	Are employees notified of their roles and responsibilities to maintain awareness and compliance with established policies, procedures, and applicable legal, statutory, or regulatory compliance obligations?	Yes	CSP-owned	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.	Compliance User Responsibility	
IAM-01.1	Are identity and access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	CSP-owned	Identity and access management policies and procedures are part of ArcGIS Online FedRAMP authorization.	Identity and Access Management Policy and Procedures	
IAM-01.2	Are identity and access management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Identity and access management policies and procedures are part of ArcGIS Online FedRAMP authorization and are reviewed and updated at least annually or if a significant change occurs.		
IAM-02.1	Are strong password policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	CSP-owned	This is a Customer Responsibility to enforce the minimum password requirements that meet their agency's security policies. Organizations should utilize ArcGIS Online Organization Specific Logins to meet all of their organizations username and password management requirements and for adherence to FedRAMP accreditation. Further information concerning ArcGIS Online Organization Specific Logins may be found at: http://doc.arcgis.com/en/arcgis-online/administer/enterprise-logins.htm If an Identity Provider (IdP) is not available. ArcGIS Online enabled Administrators to implement a custom password policy for their ArcGIS Online organization. Other than User ID lockouts which are fixed settings, password policies can be customized to meet these requirements or the specific requirements outlined in the customer's policies. For more info on setting a custom password policy, see: https://doc.arcgis.com/en/arcgis-online/administer/configure-security.htm	Strong Password Policy and Procedures	
IAM-02.2	Are strong password policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	This is a Customer Responsibility to enforce the minimum password requirements that meet their agency's security policies. ArcGIS requires passwords be changed at least annually.		
IAM-03.1	Is system identity information and levels of access managed, stored, and reviewed?	Yes	CSP-owned	User access is reviewed quarterly	Identity Inventory	
IAM-04.1	Is the separation of duties principle employed when implementing information system access?	Yes	CSP-owned	ArcGIS Online roles with corresponding information system access authorizations are defined within the ArcGIS Online Separation of Duties Matrix which as assessed annually as part of it's FedRAMP authorization	Separation of Duties	
IAM-05.1	Is the least privilege principle employed when implementing information system access?	Yes	CSP-owned	Cloud infrastructure providers utilize segregation of duties for critical functional to minimize the risk of unintentional or unauthorized access or change to production systems. Customers retain the ability to manage segregation of duties of their ArcGIS Online organization resources. The use of custom roles within ArcGIS Online enables permissions of specific user groups to be applied with much more granularity than the default roles of Administrator, Publisher, and User. For additional information, see: http://doc.arcgis.com/en/arcgis-online/reference/roles.htm	Least Privilege	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control Title	CCM Domain Title
IAM-06.1	Is a user access provisioning process defined and implemented which authorizes, records, and communicates data and assets access changes?	Yes	CSP-owned	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.	User Access Provisioning	Identity & Access Management
IAM-07.1	Is a process in place to de-provision or modify the access, in a timely manner, of movers / leavers or system identity changes, to effectively adopt and communicate identity and access management policies?	Yes	CSP-owned	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. The customer manages access provisioning and deprovisioning	User Access Changes and Revocation	
IAM-08.1	Are reviews and revalidation of user access for least privilege and separation of duties completed with a frequency commensurate with organizational risk tolerance?	Yes	CSP-owned	Customers manage access to their ArcGIS Online org	User Access Review	
IAM-09.1	Are processes, procedures, and technical measures for the segregation of privileged access roles defined, implemented, and evaluated such that administrative data access, encryption, key management capabilities, and logging capabilities are distinct and separate?	Yes	CSP-owned	Customers manage access to their ArcGIS Online org	Segregation of Privileged Access Roles	
IAM-10.1	Is an access process defined and implemented to ensure privileged access roles and rights are granted for a limited period?	Yes	CSP-owned	ArcGIS Online operations team maintains records of access control grants to all personnel. Periodic access control audits are conducted as per the FedRAMP requirements. 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.	Management of Privileged Access Roles	
IAM-10.2	Are procedures implemented to prevent the culmination of segregated privileged access?	NA	CSP-owned	Cloud infrastructure providers utilize segregation of duties for critical functional to minimize the risk of unintentional or unauthorized access or change to production systems. Customers retain the ability to manage segregation of duties of their ArcGIS Online organization resources. The use of custom roles within ArcGIS Online enables permissions of specific user groups to be applied with much more granularity than the default roles of Administrator, Publisher, and User. For additional information, see: http://doc.arcgis.com/en/arcgis-online/reference/roles.htm		
IAM-11.1	Are processes and procedures for customers to participate, where applicable, in granting access for agreed, high risk as (defined by the organizational risk assessment) privileged access roles defined, implemented and evaluated?	Yes	CSP-owned	Customers manage access to their ArcGIS Online org entirely.	CSCs Approval for Agreed Privileged Access Roles	
IAM-12.1	Are processes, procedures, and technical measures to ensure the logging infrastructure is "read-only" for all with write access (including privileged access roles) defined, implemented, and evaluated?	Yes	CSP-owned	ArcGIS Online Infrastructure read-only logs are maintained by the Software Security and Privacy team.	Safeguard Logs Integrity	
IAM-12.2	Is the ability to disable the "read-only" configuration of logging infrastructure controlled through a procedure that ensures the segregation of duties and break glass procedures?	Yes	CSP-owned	ArcGIS Online Infrastructure read-only logs are maintained by the Software Security and Privacy team.		

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control Title	CCM Domain Title
IAM-13.1	Are processes, procedures, and technical measures that ensure users are identifiable through unique identification (or can associate individuals with user identification usage) defined, implemented, and evaluated?	Yes	CSP-owned	Customers have the responsibility to grant access to their ArcGIS Online organization. All ArcGIS Online administration personnel are required to have a unique user ID and password to access the system as shared accounts are not leveraged. In order to use administration credentials multifactor authentication is utilized to uniquely identify credentials.	Uniquely Identifiable Users	
IAM-14.1	Are processes, procedures, and technical measures for authenticating access to systems, application, and data assets including multifactor authentication for a least-privileged user and sensitive data access defined, implemented, and evaluated?	Yes	CSP-owned	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	Strong Authentication	
IAM-14.2	Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted?	Yes	CSP-owned	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-15.1	Are processes, procedures, and technical measures for the secure management of passwords defined, implemented, and evaluated?	Yes	CSP-owned	Organizations should utilize ArcGIS Online Organization Specific Logins to meet all of their organizations username and password management requirements and for adherence to FedRAMP accreditation. Further information concerning ArcGIS Online Organization Specific Logins may be found at: http://doc.arcgis.com/en/arcgis-online/administer/enterprise-logins.htm If an Identity Provider (IdP) is not available. ArcGIS Online enabled Administrators to implement a custom password policy for their ArcGIS Online organization. Other than User ID lockouts which are fixed settings, password policies can be customized to meet these requirements or the specific requirements outlined in the customer's policies. For more info on setting a custom password policy, see: https://doc.arcgis.com/en/arcgis-online/administer/configure-security.htm	Passwords Management	
IAM-16.1	Are processes, procedures, and technical measures to verify access to data and system functions authorized, defined, implemented, and evaluated?	Yes	CSP-owned	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.	Authorization Mechanisms	
IPY-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for communications between application services (e.g., APIs)?	Yes	CSP-owned	The ArcGIS Online REST API is publicly available and documented on the website at: https://doc.arcgis.com/en/arcgis-online/reference/develop-with-agol.htm . Significant changes are assessed as part of a Significant Impact Assessment process to ensure appropriate evaluation, approvals and communication.	Interoperability and Portability Policy and Procedures	Interoperability & Portability
IPY-01.2	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability?	Yes	CSP-owned	See the ArcGIS Trust Center and ArcGIS Online documentation for details concerning information processing interoperability of our services - https://doc.arcgis.com/en/arcgis-online/manage-data/data-in-online.htm		
IPY-01.3	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?	Yes	CSP-owned	ArcGIS Online development code is designed to be portable in other CSP environments.		
IPY-01.4	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information/data exchange, usage, portability, integrity, and persistence?	Yes	CSP-owned	See the ArcGIS Trust Center and ArcGIS Online documentation for details concerning information processing interoperability of our services - https://doc.arcgis.com/en/arcgis-online/manage-data/data-in-online.htm		
IPY-01.5	Are interoperability and portability policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies and procedures are reviewed and updated annually or if there are any significant changes.		

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control Title	CCM Domain Title
IPY-02.1	Are CSCs able to programmatically retrieve their data via an application interface(s) to enable interoperability and portability?	Yes	CSC-owned	ArcGIS Online has extensive API capabilities allowing customers to programmatically retrieve their data. See the ArcGIS Trust Center and ArcGIS Online documentation for details concerning information processing interoperability of our services - https://doc.arcgis.com/en/arcgis-online/manage-data/data-in-online.htm	Application Interface Availability	
IPY-03.1	Are cryptographically secure and standardized network protocols implemented for the management, import, and export of data?	Yes	CSP-owned	ArcGIS Online implements FIPS 140-2 compliant cryptographic algorithms	Secure Interoperability and Portability Management	
IPY-04.1	Do agreements include provisions specifying CSC data access upon contract termination, and have the following? a. Data format b. Duration data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy	Yes	CSP-owned	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.	Data Portability Contractual Obligations	
IVS-01.1	Are infrastructure and virtualization security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Cloud infrastructure providers virtualization technologies are regularly evaluated internally and by independent assessments annually.	Infrastructure and Virtualization Security Policy and Procedures	Infrastructure & Virtualization Security
IVS-01.2	Are infrastructure and virtualization security policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Cloud infrastructure providers virtualization technologies are regularly evaluated internally and by independent assessments annually.		
IVS-02.1	Is resource availability, quality, and capacity planned and monitored in a way that delivers required system performance, as determined by the business?	Yes	CSP-owned	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	Capacity and Resource Planning	
IVS-03.1	Are communications between environments monitored?	Yes	CSP-owned	All access to the infrastructure is monitored, tracked and recorded	Network Security	
IVS-03.2	Are communications between environments encrypted?	Yes	CSP-owned	Data is encrypted at rest with AES-256 which is a FIPS 140-2 compliant encryption algorithms. This is in alignment with FedRAMP requirements		
IVS-03.3	Are communications between environments restricted to only authenticated and authorized connections, as justified by the business?	Yes	CSP-owned	ArcGIS Online data in transit is over HTTPS via TLS 1.2 Only.		
IVS-03.4	Are network configurations reviewed at least annually?	Yes	CSP-owned	All ArcGIS Online architectural diagrams (Networks and systems combined) are reviewed in accordance to the FedRAMP requirements. Updates to the diagrams are done as needed usually upon approval for architectural changes		
IVS-03.5	Are network configurations supported by the documented justification of all allowed services, protocols, ports, and compensating controls?	Yes	CSP-owned	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		
IVS-04.1	Is every host and guest OS, hypervisor, or infrastructure control plane hardened (according to their respective best practices) and supported by technical controls as part of a security baseline?	NA	CSP-owned	ArcGIS Online is a SaaS offering	OS Hardening and Base Controls	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control Title	CCM Domain Title
IVS-05.1	Are production and non-production environments separated?	Yes	CSP-owned	ArcGIS Online utilizes separate production and non-production environments. Customers can purchase a separate non-production organization for testing/staging purposes.	Production and Non-Production Environments	
IVS-06.1	Are applications and infrastructures designed, developed, deployed, and configured such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented, segregated, monitored, and restricted from other tenants?	Yes	CSP-owned	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.	Segmentation and Segregation	
IVS-07.1	Are secure and encrypted communication channels including only up-to-date and approved protocols used when migrating servers, services, applications, or data to cloud environments?	Yes	CSP-owned	ArcGIS Online enforces using only TLS 1.2 for encrypted communication with customer systems. Endpoints are regularly validated against SSL Labs and dynamic scanners to ensure the encryption is in alignment with current industry recommendations.	Migration to Cloud Environments	
IVS-08.1	Are high-risk environments identified and documented?	Yes	CSP-owned	See ArcGIS Online security presentation materials within the ArcGIS Trust Center documents.	Network Architecture Documentation	
IVS-09.1	Are processes, procedures, and defense-in-depth techniques defined, implemented, and evaluated for protection, detection, and timely response to network-based attacks?	Yes	Shared CSP and 3rd-party	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	Network Defense	
LOG-01.1	Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Logging and monitoring policies are part of the FedRAMP program and reviewed annually. All policies are maintained in a centralized location that is accessible by employees.	Logging and Monitoring Policy and Procedures	
LOG-01.2	Are policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Polices and procedures are reviewed annually as part of our FedRAMP authorization		
LOG-02.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention?	Yes	CSP-owned	Audit logs are retained as defined by ArcGIS online retention policy which is in alignment with FedRAMP requirements.	Audit Logs Protection	
LOG-03.1	Are security-related events identified and monitored within applications and the underlying infrastructure?	Yes	CSP-owned	Audit logs are reviewed weekly within the ArcGIS Online solution by the Security team	Security Monitoring and Alerting	
LOG-03.2	Is a system defined and implemented to generate alerts to responsible stakeholders based on security events and their corresponding metrics?	Yes	CSP-owned	Esri security team reviews infrastructure logs weekly. Customers are responsible for monitoring their own activity logs which include user logs and activities.		
LOG-04.1	Is access to audit logs restricted to authorized personnel, and are records maintained to provide unique access accountability?	Yes	CSP-owned	Esri security team and each customer has access to their own organizational audit logs.	Audit Logs Access and Accountability	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control Title	CCM Domain Title
LOG-05.1	Are security audit logs monitored to detect activity outside of typical or expected patterns?	Yes	CSP-owned	Audit logs are reviewed weekly within the ArcGIS Online solution by the Security team. Customers re responsible for reviewing their organizational audit logs.	Audit Logs Monitoring and Response	Logging and Monitoring
LOG-05.2	Is a process established and followed to review and take appropriate and timely actions on detected anomalies?	Yes	CSP-owned	Audit logs are reviewed weekly within the ArcGIS Online solution by the Security team. Customers re responsible for reviewing their organizational audit logs.		
LOG-06.1	Is a reliable time source being used across all relevant information processing systems?	Yes	CSP-owned	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.	Clock Synchronization	
LOG-07.1	Are logging requirements for information meta/data system events established, documented, and implemented?	Yes	CSP-owned	Data logging in alignment with NIST standards	Logging Scope	
LOG-07.2	Is the scope reviewed and updated at least annually, or whenever there is a change in the threat environment?	Yes	CSP-owned	Esri has a formal company security policy which addresses the audit and accountability requirements which includes logging. Associated procedures are updated at least annually. AGO weekly log reviews are conducted as part of the continuous monitoring activities which also includes an annual review or when there is a change in the environment.		
LOG-08.1	Are audit records generated, and do they contain relevant security information?	Yes	CSP-owned	ArcGIS Online audit records are generated in alignment with FedRAMP Moderate requirements which include ensuring they contain: successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes.	Log Records	
LOG-09.1	Does the information system protect audit records from unauthorized access, modification, and deletion?	Yes	CSP-owned	Only accessible by the ArcGIS Online infrastructure administrators	Log Protection	
LOG-10.1	Are monitoring and internal reporting capabilities established to report on cryptographic operations, encryption, and key management policies, processes, procedures, and controls?	Yes	CSP-owned	Key management policies, procedures, and processes for ArcGIS Online align with FedRAMP requirements.	Encryption Monitoring and Reporting	
LOG-11.1	Are key lifecycle management events logged and monitored to enable auditing and reporting on cryptographic keys' usage?	Yes	CSP-owned	Logging is enabled for auditing and reporting cryptographic key usage via the cloud native key management systems.	Transaction/Activity Logging	
LOG-12.1	Is physical access logged and monitored using an auditable access control system?	Yes	Shared CSP and 3rd-party	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/	Access Control Logs	
LOG-13.1	Are processes and technical measures for reporting monitoring system anomalies and failures defined, implemented, and evaluated?	Yes	CSP-owned	ArcGIS Online has developed a system configuration baseline in alignment with industry best practices such as CIS benchmarks and DISA STIGS.	Failures and Anomalies Reporting	
LOG-13.2	Are accountable parties immediately notified about anomalies and failures?	Yes	CSP-owned	Issues affecting ArcGIS Online operations are posted to the ArcGIS Trust Center Health Dashboard for ArcGIS Online here: https://trust.arcgis.com/en/system-status/		

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control Title	CCM Domain Title
SEF-01.1	Are policies and procedures for security incident management, e-discovery, and cloud forensics established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Incident management is delineated within ArcGIS Online's Incident Response Plan documentation aligning with FedRAMP requirements.	Security Incident Management Policy and Procedures	Security Incident Management, E-Discovery, & Cloud Forensics
SEF-01.2	Are policies and procedures reviewed and updated annually?	Yes	CSP-owned	Incident response plan is tested and reviewed annually		
SEF-02.1	Are policies and procedures for timely management of security incidents established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	ArcGIS Online Incident Response plan is in alignment with the FedRAMP requirements.	Service Management Policy and Procedures	
SEF-02.2	Are policies and procedures for timely management of security incidents reviewed and updated at least annually?	Yes	CSP-owned	ArcGIS Online Incident Response plan is in alignment with the FedRAMP requirements and reviewed annually.		
SEF-03.1	Is a security incident response plan that includes relevant internal departments, impacted CSCs, and other business-critical relationships (such as supply-chain) established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	ArcGIS Online Incident Response plan is in alignment with FedRAMP requirements.	Incident Response Plans	
SEF-04.1	Is the security incident response plan tested and updated for effectiveness, as necessary, at planned intervals or upon significant organizational or environmental changes?	Yes	CSP-owned	ArcGIS Online tests the Contingency and Incident Response Plans annually (at a minimum) in alignment with FedRAMP requirements.	Incident Response Testing	
SEF-05.1	Are information security incident metrics established and monitored?	Yes	CSP-owned	The ArcGIS Online Incident Response plan is in alignment with FedRAMP requirements and its effectiveness is measured using metrics that are tracked and monitored and regularly reviewed.	Incident Response Metrics	
SEF-06.1	Are processes, procedures, and technical measures supporting business processes to triage security-related events defined, implemented, and evaluated?	Yes	CSP-owned	Esri maintains a Product Security Incident Response Team (PSIRT) to manage security incidents using the FIRST PSIRT services framework to guide processes related to the intake, validation, and prioritization of security related events.	Event Triage Processes	
SEF-07.1	Are processes, procedures, and technical measures for security breach notifications defined and implemented?	Yes	CSP-owned	Impacted customers are notified within 72 of confirmed breach	Security Breach Notification	
SEF-07.2	Are security breaches and assumed security breaches reported (including any relevant supply chain breaches) as per applicable SLAs, laws, and regulations?	Yes	CSP-owned	Impacted customers are notified within 72 of confirmed breach.		
SEF-08.1	Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities?	Yes	CSP-owned	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	Points of Contact Maintenance	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control Title	CCM Domain Title
STA-01.1	Are policies and procedures implementing the shared security responsibility model (SSRM) within the organization established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Managers of ArcGIS Online employees are responsible for ensuring awareness of applicable security policies and procedures for team members. A customer responsibility matrix is available for customers within the ArcGIS Trust Center to ensure alignment with FedRAMP obligations.	SSRM Policy and Procedures	Supply Chain Management, Transparency, and Accountability
STA-01.2	Are the policies and procedures that apply the SSRM reviewed and updated annually?	Yes	CSP-owned	Policies and procedures are reviewed and updated annually or in the event of significant changes.		
STA-02.1	Is the SSRM applied, documented, implemented, and managed throughout the supply chain for the cloud service offering?	Yes	CSP-owned	This is part of our Secure Development Lifecycle and reviewed and updated annually. Esri is incorporating supplementary Supply Chain security requirements from NIST 800-53 Revision 5.	SSRM Supply Chain	
STA-03.1	Is the CSC given SSRM guidance detailing information about SSRM applicability throughout the supply chain?	Yes	CSP-owned	Esri published the ArcGIS Online Customer Responsbilitiy Matrix (CRM) to the ArcGIS Trust Center documents.	SSRM Guidance	
STA-04.1	Is the shared ownership and applicability of all CSA CCM controls delineated according to the SSRM for the cloud service offering?	Yes	CSP-owned	Responsibilities are delineated within the ArcGIS Online Customer Responsibility Matrix (CRM).	SSRM Control Ownership	
STA-05.1	Is SSRM documentation for all cloud services the organization uses reviewed and validated?	Yes	CSP-owned	This is part of our Secure Development Lifecycle and reviewed and updated annually	SSRM Documentation Review	
STA-06.1	Are the portions of the SSRM the organization is responsible for implemented, operated, audited, or assessed?	Yes	CSP-owned	ArcGIS Online has established a formal, periodic audit program that includes continual, independent internal and external assessments to validate the implementation and operating effectiveness of the ArcGIS Online control environment.	SSRM Control Implementation	
STA-07.1	Is an inventory of all supply chain relationships developed and maintained?	Yes	CSP-owned	A supplier inventory is maintained to ensure validation adherence with ArcGIS Online security and operational standards. As part of ArcGIS Online operations there are no subcontractors authorized by Esri to view any customer owned content that you upload into ArcGIS Online.	Supply Chain Inventory	
STA-08.1	Are risk factors associated with all organizations within the supply chain periodically reviewed by CSPs?	Yes	CSP-owned	Risk factors and associated assurance materials are reviewed for suppliers at least annually.	Supply Chain Risk Management	
STA-09.1	Do service agreements between CSPs and CSCs (tenants) incorporate at least the following mutually agreed upon provisions and/or terms? • Scope, characteristics, and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third-party assessment • Service termination • Interoperability and portability requirements • Data privacy	Yes	CSP-owned	ArcGIS Online's Terms of use are available within the ArcGIS Trust Center documents tab: https://www.esri.com/content/dam/esrisites/en-us/media/legal/ma-translations/english.pdf	Primary Service and Contractual Agreement	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control Title	CCM Domain Title
STA-10.1	Are supply chain agreements between CSPs and CSCs reviewed at least annually?	Yes	CSP-owned	ArcGIS Online third party agreement processes include periodic review and reporting, and are reviewed by independent auditors.	Supply Chain Agreement Review	
STA-11.1	Is there a process for conducting internal assessments at least annually to confirm the conformance and effectiveness of standards, policies, procedures, and SLA activities?	Yes	CSP-owned	ArcGIS Online has established a formal, periodic audit program that includes continual, independent internal and annual external assessments to validate the implementation and operating effectiveness of the ArcGIS Online control environment.	Internal Compliance Testing	
STA-12.1	Are policies that require all supply chain CSPs to comply with information security, confidentiality, access control, privacy, audit, personnel policy, and service level requirements and standards implemented?	Yes	CSP-owned	This is part of our Secure Development Lifecycle and agreements are reviewed annually	Supply Chain Service Agreement Compliance	
STA-13.1	Are supply chain partner IT governance policies and procedures reviewed periodically?	Yes	CSP-owned	This is part of our Secure Development Lifecycle and agreements are reviewed annually	Supply Chain Governance Review	
STA-14.1	Is a process to conduct periodic security assessments for all supply chain organizations defined and implemented?	Yes	CSP-owned	An annual assessment is conducted of the entire ArcGIS Online solution including Supply Chain organizations, in alignment with FedRAMP requirements	Supply Chain Data Security Assessment	
TVM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to identify, report, and prioritize the remediation of vulnerabilities to protect systems against vulnerability exploitation?	Yes	CSP-owned	Priority of addressing vulnerabilities in alignment with FedRAMP requirements.	Threat and Vulnerability Management Policy and Procedures	
TVM-01.2	Are threat and vulnerability management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	In alignment with FedRAMP requirements threat detection signatures and behavioral analysis tools used or installed on systems in ArcGIS Online are updated frequently		
TVM-02.1	Are policies and procedures to protect against malware on managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	All systems in ArcGIS Online as well as administrator workstations have anti-malware installed. This is in alignment to FedRAMP requirements.	Malware Protection Policy and Procedures	
TVM-02.2	Are asset management and malware protection policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	In alignment with FedRAMP requirements threat detection signatures and behavioral analysis tools used or installed on systems in ArcGIS Online are updated frequently		
TVM-03.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable scheduled and emergency responses to vulnerability identifications (based on the identified risk)?	Yes	CSP-owned	This is part of our Continuous Monitoring as part of our FedRAMP authorization. Esri's Software Security & Privacy team notifies and coordinates with the appropriate Operations Teams when conducting security-related activities within the system boundary. Activities include, vulnerability scanning, contingency testing, and incident response exercises. ArcGIS Online performs external vulnerability scans at least monthly and identified issues are investigated and tracked to resolution - This is performed annually by a third party assessor against FedRAMP moderate controls, including the addition of pentesting. ArcGIS Online also addressing Emergency Operational Directives as they are issued.	Vulnerability Remediation Schedule	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control Title	CCM Domain Title
TVM-04.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to update detection tools, threat signatures, and compromise indicators weekly (or more frequent) basis?	Yes	CSP-owned	In alignment with FedRAMP requirements threat detection signatures and behavioral analysis tools used or installed on systems in ArcGIS Online are updated frequently	Detection Updates	Threat & Vulnerability Management
TVM-05.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to identify updates for applications that use third-party or open-source libraries (according to the organization's vulnerability management policy)?	Yes	CSP-owned	Vulnerability assessments against ArcGIS Online are conducted at least monthly as part of the Continuous Monitoring Plan - including system, web application and database scans.	External Library Vulnerabilities	
TVM-06.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for periodic, independent, third-party penetration testing?	Yes	CSP-owned	Penetration testing is done through our SAA process.	Penetration Testing	
TVM-07.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly?	Yes	CSP-owned	Vulnerability assessments against ArcGIS Online are conducted at least monthly as part of the Continuous Monitoring Plan - including system, web application and database scans.	Vulnerability Identification	
TVM-08.1	Is vulnerability remediation prioritized using a risk-based model from an industry-recognized framework?	Yes	CSP-owned	Vulnerability assessments against ArcGIS Online are conducted at least monthly as part of the Continuous Monitoring Plan - including system, web application and database scans. Issues are categorized by adjusted CVSS scores to reflect operational risk and remediated in alignment with FedRAMP Moderate timelines: HIGH risk - within 30 days, MODERATE risk - within 90 days, and LOW risk - within 180 days. Critical risk issues are addressed in less then 7 days.	Vulnerability Prioritization	
TVM-09.1	Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification?	Yes	CSP-owned	See - TVM-08.1 - The ArcGIS Online Continuous Monitoring Plan (in alignment with FedRAMP Moderate control requirements) ensures appropriate tracking and reporting of vulnerabilities through a Plan of Actions and Milestones (POAM) listing. Issues are discussed with authorized resources as part of monthly ConMon meetings.	Vulnerability Management Reporting	
TVM-10.1	Are metrics for vulnerability identification and remediation established, monitored, and reported at defined intervals?	Yes	CSP-owned	This is part of our Continuous Monitoring as part of our FedRAMP authorization. Vulnerability scans occur at least monthly and metrics are summarized and discussed as part of the monthly ConMon meeting,	Vulnerability Management Metrics	
UEM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for all endpoints?	Yes	CSP-owned	Customers are responsible for establishing, documenting and maintaining policies and procedures for endpoints.	Endpoint Devices Policy and Procedures	
UEM-01.2	Are universal endpoint management policies and procedures reviewed and updated at least annually?	NA	CSP-owned	Customers are responsible for updating policies and procedures for universal endpoint.		
UEM-02.1	Is there a defined, documented, applicable and evaluated list containing approved services, applications, and the sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data?	NA	CSC-owned	Customers are responsible for maintaining an internal software solution with the approved list of applications that can be installed on managed endpoints based on OS	Application and Service Approval	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control Title	CCM Domain Title
UEM-03.1	Is a process defined and implemented to validate endpoint device compatibility with operating systems and applications?	NA	CSP-owned	Customers are responsible for validating endpoint device compatibility with OS and Applications.	Compatibility	Universal Endpoint Management
UEM-04.1	Is an inventory of all endpoints used and maintained to store and access company data?	NA	CSC-owned	Customers are responsible for maintaining a centralized inventory system for all managed endpoints which ingests data from various inventory systems to prevent duplicates.	Endpoint Inventory	
UEM-05.1	Are processes, procedures, and technical measures defined, implemented and evaluated, to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data?	Yes	CSP-owned	Customers are responsible for defining, implementing and evaluating technical measures, that enforce policies and controls for all endpoints access.	Endpoint Management	
UEM-06.1	Are all relevant interactive-use endpoints configured to require an automatic lock screen?	Yes	Shared CSP and CSC	AGO system configuration implements an automatic screen lock after a pre-defined period of time of inactivity. Customers are responsible for ensuring lockscreens are enabled for their workstations.	Automatic Lock Screen	
UEM-07.1	Are changes to endpoint operating systems, patch levels, and/or applications managed through the organizational change management process?	Yes	CSP-owned	Customers are responsible maintaining changes to the endpoint OS and/or application.	Operating Systems	
UEM-08.1	Is information protected from unauthorized disclosure on managed endpoints with storage encryption?	NA	CSC-owned	Customers are responsible for all their managed endpoints to be encrypted based on their organizational security requirements	Storage Encryption	
UEM-09.1	Are anti-malware detection and prevention technology services configured on managed endpoints?	Yes	CSP-owned	Customers are responsible implementing anti-malware detection and prevention technology services on customer managed endpoints.	Anti-Malware Detection and Prevention	
UEM-10.1	Are software firewalls configured on managed endpoints?	Yes	CSP-owned	Esri assets (e.g. laptops) are configured with anti-virus software that includes e-mail filtering, software firewalls, and malware detection.	Software Firewall	
UEM-11.1	Are managed endpoints configured with data loss prevention (DLP) technologies and rules per a risk assessment?	NA	Shared CSP and CSC	ArcGIS Online customers are responsible for the management of the data they place into ArcGIS Online. Esri has no insight as to what type of content the customer chooses to store in ArcGIS Online and the customer retains complete control of how they choose to classify their content, where it is stored, used and protected from disclosure.	Data Loss Prevention	
UEM-12.1	Are remote geolocation capabilities enabled for all managed mobile endpoints?	No	CSP-owned	Not utilized	Remote Locate	
UEM-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices?	NA	CSC-owned	Customers are responsible for policies and procedures for mobile device security which reserves the right to remotely wipe mobile devices.	Remote Wipe	
UEM-14.1	Are processes, procedures, and technical and/or contractual measures defined, implemented, and evaluated to maintain proper security of third-party endpoints with access to organizational assets?	NA	CSP-owned	Customers are responsible implementing processes, procedures and technical measures evaluating security of third-party endpoints.	Third-Party Endpoint Security Posture	
End of Standard						

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control Title	CCM Domain Title

Summary of answer fields:

Assessment Question

The description of the question.			

CSP CAIQ Answer

The Cloud Service Provider (CSP) must respond with "Yes"/ "No"/ "NA" next to the corresponding assessment question, and for the portion(s) of the CCM control specification they are responsible and accountable for implementing.

Meaning of possible replies:

• "Yes": The portion(s) of the CCM control requirement corresponding to the assessment question is met.

• "No": The portion(s) of the CCM control requirement corresponding to the assessment question is not met.

• "N/A": The question is not in scope and does not apply to the cloud service under assessment.

NOTES:

A "Yes" answer ii

A "No" answer indicates that the portion of the control in question is not implemented, while in scope of the assessment. The CSP has to assign the implementation responsibility of the control to the relevant party under column "SSRM control ownership"

A "N/A" answer indicates that the portion of the control in question is out of scope of the assessment. The "SSRM control ownership" column is to be left blank (e.g., greyed out), and optionally the CSP may explain why it is the case

Shared Security Responsibility Model (SSRM) control ownership

The CSP control responses shall identify control applicability and ownership for their specific service.

• CSP-owned: The CSP is entirely responsible and accountable for the CCM control implementation.

• CSC-owned: The Cloud Service Customer (CSC) is entirely responsible and accountable for the CCM control implementation.

• Third-party outsourced: The third-party CSP in the supply chain (e.g., an IaaS provider) is responsible for CCM control implementation, while the CSP is fully accountable.

• Shared CSP and CSC: Both the CSP and CSC share CCM control implementation responsibility and accountability.

• Shared CSP and third party: Any CCM control implementation responsibility is shared between CSP and the third party, but the CSP remains fully accountable.

Note: The CAIQv4 SSRM schema is tailored to CCMv4's Supply Chain Management, Transparency, and Accountability (STA) domain, controls 1-6, and their corresponding implementation guidelines.

CSP implementation description (optional/recommended)

A description (with references) of how the cloud service provider meets (or does not meet) the portion(s) of the SSRM control they are responsible for. If "NA," explain why.