ArcGIS Online FedRAMP Moderate Customer Responsibility Matrix (CRM) Worksheet

Control ID	Specific Inheritance and Customer Agency/CSP Responsibilities
AC-3	Customers are responsible for managing access to their AGO Organization and for managing the AGO roles defined and any custom roles that are created by that Customer. Customer is also responsible for providing a SAML 2.0 Identity Provider for identity integration with the application, according to their policies and procedures to meet authentication requirements.
AC-8 (a)	Customers are responsible for adhering to all organizational policies and procedures in regard to displaying their system use notification banner. AGO allows customers to inject any banners or branding they might require at the application tier
AC-8 (c)	Customers are responsible for displaying system use information before granting further access to the publicly accessible resources in ArcGIS Online. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities and including a description of the authorized uses of the system. NOTE: If the customer has no publicly accessing resources in ArcGIS Online, then this control can be inherited from the CSP.
AC-14 (a)	Customer is responsible for identifying actions that can be performed on the customer-deployed resources without identification or authentication (e.g., such as viewing a publicly accessible services or apps or form).
AC-14 (b)	Customer is responsible for providing documentation for user actions not requiring identification or authentication in the customer organization. It is the responsibility of the customer to follow their own Rules of Behavior and policies around inviting and sharing to guests to application.
AC-21 (b)	The customer is responsible for employing a process to assist users with making information sharing decisions
AC-22 (a)	Customer is responsible for designating authorized personnel to post publicly accessible information in their AGO application.
AC-22 (b)	Customer is responsible for training the personnel defined in AC-21. a to prevent disclosure of nonpublic customer-controlled information.
AC-22 (c)	Customer is responsible for reviewing proposed content of customer-controlled information prior to posting publicly to ensure nonpublic information is not included.
AC-22 (d)	Customer is responsible for periodically reviewing publicly available customer-controlled content for nonpublic information.
AT-2 (a)	Customer is responsible providing training for their users, training may be developed using the AGO user guide and other online documentations.
AT-2 (b)	Customer is responsible providing training for their users, training may be developed using the AGO user guide and other online documentations.
AT-2 (c)	Customer is responsible providing training for their users, training may be developed using the AGO user guide and other online documentations.
AT-2 (d)	Customer is responsible providing training for their users, training may be developed using the AGO user guide and other online documentations.
AT-2(2)	Customer is responsible providing training for their users, training may be developed using the AGO user guide and other online documentations.
AT-2(3)	Customer is responsible providing training for their users, training may be developed using the AGO user guide and other online documentations.
AT-3 (a)	Customer is responsible providing training for their users, training may be developed using the AGO user guide and other online documentations.
AT-3 (b)	Customer is responsible providing training for their users, training may be developed using the AGO user guide and other online documentations.
AT-3 (c)	Customer is responsible providing training for their users, training may be developed using the AGO user guide and other online documentations.
AT-4 (a)	Customer is responsible for retaining the training records for their users.
AT-4 (b)	Customer is responsible for retaining the training records for their users.
CA-6 (a)	Sponsoring agency must identify a senior-level executive or manager as the authorizing official for the AGO.
CA-6 (b)	Agency must also determine whether the risk to the agency is acceptable. Following review of the security authorization package and discussing with agency officials and Independent Assessor/3PAO, the AO renders an authorization.
CA-6 (c)	Authorizing official for the system, are responsible for ensuring authorization before commencing operations
CA-6 (d)	Authorizing official is responsible for ensuring that for common controls for inheritance by organizational systems are authorized
CA-6 (e)	Authorizing official agency is responsible for updating the authorizaiton in accordance with OMB A-130 requirements or when a significant change occurs
CP-9 (a)	Customer is responsible for conducting backups of user-level information in customer-deployed resources at a frequency consistent with customer-defined RTOs and RPOs.
CP-9 (d)	Customer is responsible for protecting the confidentiality, integrity, and availability of backup information they backed up.
CP-9(1)	Customer is responsible for backing up customer data and applications they developed. Customer is also responsible for testing those backups.
IA-2	Customer is responsible for providing a SAML 2.0 configuration to federate their ArcGIS Online organization with their agency identity provider for authentication.
IA-2(1)	Customers are responsible for MFA implementation against their Identity provide for integration with AGO. AGO supports any SAML 2.0 compatible Identity Provider via Organization-specific logins.
IA-2(2)	Customer or agency is responsible for implementing multifactor user accounts for their ArcGIS Online application users using any SAML 2.0 compliant identity provider
IA-2(5)	Customer is responsible for requiring individuals using group authenticators to first authenticate using individual authenticators
IA-2(8)	Customer is responsible for accepting and electronically verifying Federal Identify, Credential and Access Management-FICAM approved third-party credentials
IA-2(12)	Customers using any SAML 2.0 compliant Identify provider (IdP) are responsible for accepting and electronically verifying Personal Identity Verification (PIV) credentials for customer users
IA-3	Customers are required to ensure their information systems uniquely identify and authenticate approved device types prior to establishing a connection with AGO
IA-5 (a)	Customer is responsible for provisioning and managing their users and authenticators in accordance with their organization's security requirements or per FedRAMP guidance.
IA-5 (b)	Customers using identity federation, are responsible for federal/customer user authenticator content.
IA-5 (c)	Customers using identity federation, are responsible for federal/customer user authenticator content and password strength.
IA-5 (d)	Customers using identity federation, are responsible for federal/customer user authenticator management and content.
IA-5 (e)	Customer is responsible for managing their authenticators, including changing default content of authenticators prior to deployment.

Control ID	Specific Inheritance and Customer Agency/CSP Responsibilities
IA-5 (f)	Customer is responsible for managing their authenticators, including the establishment of minimum and maximum lifetime restrictions and reuse conditions for authenticators.
IA-5 (g)	Customer is responsible for managing their authenticators, including changing and refreshing authenticators, and the corresponding time after which an update is required for each authenticator type.
IA-5 (h)	Customer is responsible for managing and protecting their authenticator content from unauthorized disclosure and modification.
IA-5 (i)	Customer is responsible for managing their authenticators, including implementing and specifying security safeguards to protect authenticators.
IA-5(2)	Customer is responsible for managing their users and authenticators to align with their organization's PKI implementation requirements or in accordance with FedRAMP guidance
IA-5(6)	Customer is responsible for protecting authenticators commensurate with the security category of the information to which use of the authenticator permits access.
IA-5(7)	Customers are responsible for ensuring that they do not store authenticators for their organizational users in scripts or function keys or embed them in applications.
IA-8	Government customers are responsible for identifying and authenticating non-organizational users accessing the agency's application
IA-8(1)	Government customers are responsible for supplying a SAML 2.0 compatible identity provider (IdP) that supports and accepts electronically verifying Personal Identity Verification (PIV) credentials.
IA-8(2)	Government customers using SAML 2.0 compliant IdPs are responsible for ensuring it is configured to utilize external authenticators that are NIST compliant and maintaining a list of accepted external authenticators.
IA-8(4)	Government customers are responsible for use of defined profiles conforming their organization's requirements.
IA-11	Customers configure SAML authentication in alignment with their organization-defined circumstances or situations requiring re-authentication
IR-4 (a)	Government customers are responsible for subscribing to AGO information feeds to learn of incidents that may impact their operations. These feeds include the ArcGIS Trust Center RSS feed, which is an automated method to be made aware of AGO issues and related guidance.
IR-9 (a)	Government customers are responsible for responsible for developing policies and procedures for managing information spills resulting from actions under the customer's direct control.
IR-9 (b)	Government customers are responsible for responsible for developing policies and procedures to identify the specific information spilled as a result of actions under the customer's direct control.
IR-9 (c)	Government customers are responsible for responsible for developing policies and procedures for managing communication regarding information spills resulting from actions under the customer's direct control.
IR-9(2)	Government customers are responsible for training personnel or roles per their information spillage policy using a method of communication not associated with the spill.
SC-8	Customers are responsible for ensuring that their client software is configured to only establish sessions using FIPS 140-2 compliant protocols.
SC-13 (a)	Government customers are responsible for ensuring that their client software is configured to only establish sessions using FIPS 140-2 compliance protocols. This can be accomplished by restricting access to the government customer's internal network traffic.
SC-13 (b)	Government customers are responsible for ensuring that their client software is configured to only establish sessions using FIPS 140-2 compliance protocols.
SR-8	Customers should subscribe to the RSS feed from the ArcGIS Trust Center