Mapping of FedRAMP Moderate Rev 5 Baseline to ISO 27001 Security Controls

This document provides a list of all controls that require the Cloud Service Provider, Esri, to provide detailed descriptions of their implementation, that meets the intent of the security requirements. All required controls are tested by an approved assessor annually. ArcGIS Online does not undergo a separate ISO 27001 certification as the FedRAMP authorization meets requirements for equivalent or better security assurance, however ISO 27001 is planned for our EU Region. This mapping is aligned to the latest version of FedRAMP Moderate / NIST SP 800-53 Revision 5 controls to ISO/IEC 27001:2022 requirements.

Revision History

Date	Description	Version	Author
6/1/2024	Initial mapping of NIST 800-53 Rev5 FedRAMP security controls in-scope of Moderate authorizations (such as ArcGIS Online) to International Standards Organization (ISO) 27001:2022 security controls. Source documents are as follows:	1	Esri
5/30/2024	FedRAMP Security Controls Moderate Baseline		FedRAMP
10/12/2023	National Online Informative References Program | CSRC (nist.gov)		NIST

MAPPING FedRAMP Moderate/NIST SP 800-53, REVISION 5 TO ISO/IEC 27001:2022

NIST SP 800-53, REVISION 5 CONTROLS		ISO/IEC 27001:2022 REQUIREMENTS AND CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control **partially satisfy** the intent of the NIST control.*
AC-1	Access Control Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.15, A.5.31, A.5.36, A.5.37
AC-2 (1) (2) (3) (4) (5) (7) (9) (12) (13)	Account Management	A.5.16, A.5.18, A.8.2
AC-3	Access Enforcement	A.5.15, A.5.33*, A.8.3, A.8.4*, A.8.18, A.8.20, A.8.26
AC-4 (21)	Information Flow Enforcement	A.5.14, A.8.22, A.8.23
AC-5	Separation of Duties	A.5.3
AC-6 (1) (2) (5) (7) (9) (10)	Least Privilege	A.5.15*, A.8.2, A.8.18
AC-7	Unsuccessful Logon Attempts	A.8.5*
AC-8	System Use Notification	A.8.5*
AC-9	Previous Logon Notification	A.8.5*
AC-10	Concurrent Session Control	None
AC-11 (1)	Device Lock	A.7.7, A.8.1
AC-12	Session Termination	None
AC-14	Permitted Actions without Identification or Authentication	None
AC-17 (1) (2) (3) (4) (9)	Remote Access	A.5.14, A.6.7, A.8.1,
AC-18 (1) (3)	Wireless Access	A.5.14, A.8.1, A.8.20
AC-19 (5)	Access Control for Mobile Devices	A.5.14, A.7.9, A.8.1
AC-20 (1) (2)	Use of External Systems	A.5.14, A.7.9, A.8.20
AC-21	Information Sharing	None
AC-22	Publicly Accessible Content	None
AT-1	Awareness and Training Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
AT-2 (2) (3)	Literacy Training and Awareness	7.3, A.6.3, A.8.7*
AT-3	Role-Based Training	A.6.3*
AT-4	Training Records	None
AU-1	Audit and Accountability Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
AU-2	Event Logging	A.8.15
AU-3 (1)	Content of Audit Records	A.8.15*
AU-4	Audit Log Storage Capacity	A.8.6
AU-5	Response to Audit Logging Process Failures	None
AU-6 (1) (3)	Audit Record Review, Analysis, and Reporting	A.5.25, A.6.8, A.8.15
AU-7 (1)	Audit Record Reduction and Report Generation	None
AU-8	Time Stamps	A.8.17
AU-9 (4)	Protection of Audit Information	A.5.33, A.8.15
AU-11	Audit Record Retention	A.5.28, A.8.15
AU-12	Audit Record Generation	A.8.15
CA-1	Assessment and Authorization Policies and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, 9.2.2*, 9.3.1*, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
CA-2 (1) (3)	Control Assessments	9.2.1*, 9.2.2*, A.5.30*, A.5.36, A.8.29
CA-3	Information Exchange	A.5.14, A.8.21
CA-5	Plan of Action and Milestones	8.3, 9.3.3*, 10.2*
CA-6	Authorization	9.3.1*, 9.3.3*
CA-7 (1) (4)	Continuous Monitoring	9.1, 9.3.2*, 9.3.3*, A.5.36*
CA-8 (1) (2)	Penetration Testing	None
CA-9	Internal System Connections	None
CM-1	Configuration Management Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37, A.8.9

NIST SP 800-53, REVISION 5 CONTROLS		ISO/IEC 27001:2022 REQUIREMENTS AND CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control **partially satisfy** the intent of the NIST control.*
CM-2 (2) (3) (7)	Baseline Configuration	A.8.9
CM-3 (2) (4)	Configuration Change Control	8.1, 9.3.3*, A.8.9, A.8.32
CM-4 (2)	Impact Analyses	A.8.9
CM-5 (1) (5)	Access Restrictions for Change	A.8.2, A.8.4, A.8.9, A.8.19, A.8.31, A.8.32
CM-6 (1)	Configuration Settings	A.8.9
CM-7 (1) (2) (5)	Least Functionality	A.8.19*
CM-8 (1) (3)	System Component Inventory	A.5.9, A.8.9
CM-9	Configuration Management Plan	A.5.2*, A.8.9
CM-10	Software Usage Restrictions	A.5.32*
CM-11	User-Installed Software	A.8.19*
CM-12 (1)	Information Location	None
CP-1	Contingency Planning Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
CP-2 (1) (3) (8)	Contingency Plan	7.5.1, 7.5.2, 7.5.3, A.5.2, A.5.29, A.8.14
CP-3	Contingency Training	A.6.3*
CP-4 (1)	Contingency Plan Testing	A.5.29, A.5.30*
CP-6 (1) (3)	Alternate Storage Site	A.5.29*, A.7.5*, A.8.14*
CP-7 (1) (2) (3)	Alternate Processing Site	A.5.29*, A.7.5*, A.8.14*
CP-8 (1) (2)	Telecommunications Services	A.5.29*, A.7.11
CP-9 (1) (8)	System Backup	A.5.29*, A.5.33*, A.8.13
CP-10 (2)	System Recovery and Reconstitution	A.5.29*
IA-1	Identification and Authentication Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
IA-2 (1) (2) (5) (6) (8) (12)	Identification and Authentication (Organizational Users)	A.5.16
IA-3	Device Identification and Authentication	None
IA-4 (4)	Identifier Management	A.5.16
IA-5 (1) (2) (6) (7)	Authenticator Management	A.5.16, A.5.17
IA-6	Authentication Feedback	A.8.5*
IA-7	Cryptographic Module Authentication	None
IA-8 (1) (2) (4)	Identification and Authentication (Non-Organizational Users)	A.5.16
IA-11	Re-authentication	None
IA-12 (2) (3) (5)	Identity Proofing	None
IR-1	Incident Response Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
IR-2	Incident Response Training	A.6.3*
IR-3 (2)	Incident Response Testing	None
IR-4 (1)	Incident Handling	A.5.25, A.5.26, A.5.27
IR-5	Incident Monitoring	None
IR-6 (1) (3)	Incident Reporting	A.5.5*, A.6.8
IR-7 (1)	Incident Response Assistance	None
IR-8	Incident Response Plan	7.5.1, 7.5.2, 7.5.3, A.5.24
IR-9 (2) (3) (4)	Information Spillage Response	None
MA-1	System Maintenance Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.37, A.18.1.1, A.18.2.2
MA-2	Controlled Maintenance	A.7.10*, A.7.13*, A.8.10*
MA-3 (1) (2) (3)	Maintenance Tools	None
MA-4	Nonlocal Maintenance	None
MA-5 (1)	Maintenance Personnel	None
MP-1	Media Protection Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
MP-2	Media Access	A.5.10*, A.7.7*, A.7.10*

NIST SP 800-53, REVISION 5 CONTROLS		ISO/IEC 27001:2022 REQUIREMENTS AND CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control **partially satisfy** the intent of the NIST control.*
MP-3	Media Marking	A.5.13
MP-4	Media Storage	A.5.10*, A.7.7*, A.7.10, A.8.10*
MP-5	Media Transport	A.5.10*, A.7.9, A.7.10
MP-6	Media Sanitization	A.5.10, A.7.10*, A.7.14, A.8.10
MP-7	Media Use	A.5.10, A.7.10
PE-1	Physical and Environmental Protection Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
PE-2	Physical Access Authorizations	A.7.2*
PE-3	Physical Access Control	A.7.1, A.7.2, A.7.3, A.7.4
PE-4	Access Control for Transmission Medium	A.7.2, A.7.12
PE-5	Access Control for Output Devices	A.7.2, A.7.3, A.7.7
PE-6 (1)	Monitoring Physical Access	A.7.4, A.8.16*
PE-8	Visitor Access Records	None
PE-9	Power Equipment and Cabling	A.7.5, A.7.8, A.7.11, A.7.12
PE-10	Emergency Shutoff	A.7.11*
PE-11	Emergency Power	A.7.11
PE-12	Emergency Lighting	A.7.11*
PE-13 (1) (2)	Fire Protection	A.7.5, A.7.8
PE-14	Environmental Controls	A.7.5, A.7.8, A.7.11
PE-15	Water Damage Protection	A.7.5, A.7.8, A.7.11
PE-16	Delivery and Removal	A.5.10*, A.7.2*, A.7.10*
PE-17	Alternate Work Site	A.5.14*, A.6.7, A.7.9
PL-1	Planning Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
PL-2	System Security and Privacy Plans	7.5.1, 7.5.2, 7.5.3, 10.2, A.5.8*
PL-4 (1)	Rules of Behavior	A.5.4, A.5.10, A.6.2*
PL-8	Security and Privacy Architectures	A.5.8*
PL-10	Baseline Selection	None
PL-11	Baseline Tailoring	None
PS-1	Personnel Security Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
PS-2	Position Risk Designation	None
PS-3 (3)	Personnel Screening	A.6.1
PS-4	Personnel Termination	A.5.11, A.6.5
PS-5	Personnel Transfer	A.5.11, A.6.5
PS-6	Access Agreements	A.5.4*, A.6.2, A.6.6*
PS-7	External Personnel Security	A.5.2, A.5.4*
PS-8	Personnel Sanctions	7.3, A.6.4
PS-9	Position Descriptions	A.5.2
RA-1	Risk Assessment Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
RA-2	Security Categorization	A.5.12*
RA-3 (1)	Risk Assessment	6.1.2, 8.2, 9.3.2*, A.8.8*
RA-5 (2) (3) (5) (11)	Vulnerability Monitoring and Scanning	A.8.8*
RA-7	Risk Response	6.1.3, 8.3, 10.2
RA-9	Criticality Analysis	A.5.22*
SA-1	System and Services Acquisition Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, 8.1, A.5.1, A.5.2, A.5.4, A.5.23, A.5.31, A.5.36, A.5.37
SA-2	Allocation of Resources	None
SA-3	System Development Life Cycle	A.5.2*, A.5.8, A.8.25, A.8.31*
SA-4 (1) (2) (9) (10)	Acquisition Process	8.1, A.5.8, A.5.20, A.5.23, A.8.29, A.8.30
SA-5	System Documentation	7.5.1, 7.5.2, 7.5.3, A.5.37*

NIST SP 800-53, REVISION 5 CONTROLS		ISO/IEC 27001:2022 REQUIREMENTS AND CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control **partially satisfy** the intent of the NIST control.*
SA-8	Security Engineering Principles	A.8.27, A.8.28*
SA-9 (1) (2) (5)	External System Services	A.5.2*, A.5.4*, A.5.8*, A.5.14*, A.5.22, A.5.23, A.8.21
SA-10	Developer Configuration Management	A.8.9, A.8.28*, A.8.30*, A.8.32
SA-11 (1) (2)	Developer Testing and Evaluation	A.8.29, A.8.30*
SA-15 (3)	Development Process, Standards, and Tools	A.5.8*, A.8.25
SA-22	Unsupported System Components	None
SC-1	System and Communications Protection Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
SC-2	Separation of System and User Functionality	None
SC-4	Information In Shared System Resources	None
SC-5	Denial-of Service-Protection	None
SC-7 (3) (4) (5) (7) (8) (12) (18)	Boundary Protection	A.5.14*, A.8.16*, A.8.20*, A.8.22*, A.8.23*, A.8.26*
SC-8 (1)	Transmission Confidentiality and Integrity	A.5.10*, A.5.14, A.8.20*, A.8.26*
SC-10	Network Disconnect	A.8.20
SC-12	Cryptographic Key Establishment and Management	A.8.24
SC-13	Cryptographic Protection	A.8.24, A.8.26, A.5.31
SC-15	Collaborative Computing Devices and Applications	A.5.14*
SC-17	Public Key Infrastructure Certificates	A.8.24
SC-18	Mobile Code	None
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	None
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	None
SC-22	Architecture and Provisioning for Name/Address Resolution Service	None
SC-23	Session Authenticity	None
SC-28 (1)	Protection of Information at Rest	A.5.10*
SC-39	Process Isolation	None
SC-45 (1)	System Time Synchronization	None
SI-1	System and Information Integrity Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
SI-2 (2) (3)	Flaw Remediation	A.6.8*, A.8.8, A.8.32*
SI-3	Malicious Code Protection	A.8.7
SI-4 (1) (2) (4) (5) (16) (18) (23)	System Monitoring	A.8.16*
SI-5	Security Alerts, Advisories, and Directives	A.5.6*
SI-6	Security and Privacy Function Verification	None
SI-7 (1) (7)	Software, Firmware, and Information Integrity	None
SI-8 (2)	Spam Protection	None
SI-10	Information Input Validation	None
SI-11	Error Handling	None
SI-12	Information Management and Retention	None
SI-16	Memory Protection	None
SR-1	Supply Chain Risk Management Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.19, A.5.31, A.5.36, A.5.37
SR-2 (1)	Supply Chain Risk Management Plan	A.5.19, A.5.20*, A.5.21*, A.8.30*
SR-3	Supply Chain Controls and Processes	A.5.20, A.5.21*
SR-5	Acquisition Strategies, Tools, and Methods	A.5.20, A.5.21, A.5.23
SR-6	Supplier Assessments and Reviews	A.5.22
SR-8	Notification Agreements	None

NIST SP 800-53, REVISION 5 CONTROLS		ISO/IEC 27001:2022 REQUIREMENTS AND CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control **partially satisfy** the intent of the NIST control.*
SR-10	Inspection of Systems or Components	None
SR-11 (1) (2)	Component Authenticity	None
SR-12	Component Disposal	None