Mapping of FedRAMP *Tailored* LI-SaaS 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, or provide a self-attestation that their implementation meets the intent of the security requirements. All required and conditional 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.

Revision History

Date	Description	Version	Author
7/20/2018	Initial mapping of NIST 800-53 Rev4 security controls in-scope of Li-SaaS authorizations (such as ArcGIS Online) to International Standards Organization (ISO) 27001 security controls. Source documents are as follows:	1	Esri Software Security & Privacy
	NIST 800-53 Rev4	1/22/2015	NIST
	FedRAMP Tailored Low Security Controls	11/14/2017	FedRAMP

FedRAMP *Tailored* LI-SaaS Baseline Mapping to ISO 27001

No	NIST 800-53 Control ID	ISO 27001 Control	NIST 800-53 Control Name	Tailoring Action	Additional Control Tailoring Comments
1	AC-1	A.5.1.1, A.5.1.2, A.6.1.1, A.9.1.1, A.12.1.1, A.18.1.1, A.18.2.2	Access Control Policy & Procedures	Attest	
2	AC-2	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6	Account Management	Document and Assess	
3	AC-3	A.6.2.2, A.9.1.2, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.1, A.14.1.2, A.14.1.3, A.18.1.3	Access Enforcement	Document and Assess	
4	AC-7	A.9.4.2	Unsuccessful Login Attempts	NSO, Attest	NSO - for non-privileged users. Attestation - for privileged users related to multi-factor identification and authentication.
5	AC-17	A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2	Remote Access	Document and Assess	
6	AC-20	A.11.2.6, A.13.1.1, A.13.2.1	Use of External Information Systems	Attest	
7	AC-22	None	Publicly Accessible Content	Document and Assess	
8	AT-1	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	Security Awareness and Training Policy and Procedures	Attest	
9	AT-2	A.7.2.2, A.12.2.1	Security Awareness Training	Attest	
10	AT-3	A.7.2.2*	Role-Based Security Training	Attest	
11	AT-4	None	Security Training Records	Attest	
12	AU-1	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	Audit and Accountability Policy and Procedures	Attest	
13	AU-2	None	Audit Events	Attest	
14	AU-3	A.12.4.1*	Content of Audit Records	Document and Assess	
15	AU-5	None	Response to Audit Processing Failures	Document and Assess	
16	AU-6	A.12.4.1, A.16.1.2, A.16.1.4	Audit Review, Analysis, and Reporting	Document and Assess	
17	AU-8	A.12.4.4	Time Stamps	Attest	
18	AU-9	A.12.4.2, A.12.4.3, A.18.1.3	Protection of Audit Information	Attest	
19	AU-12	A.12.4.1, A.12.4.3	Audit Generation	Attest	
20	CA-1	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	Security Assessment and Authorization Policies and Procedures	Attest	
21	CA-2	A.14.2.8, A.18.2.2, A.18.2.3	Security Assessments	Document and Assess	
22	CA-2 (1)	A.14.2.8, A.18.2.2, A.18.2.3	Security Assessments | Independent Assessors	Attest	

No	NIST 800-53 Control ID	ISO 27001 Control	NIST 800-53 Control Name	Tailoring Action	Additional Control Tailoring Comments
23	CA-3	A.13.1.2, A.13.2.1, A.13.2.2	System Interconnections	Document and Assess (Conditional)	Condition: There are connection(s) to external systems. Connections (if any) shall be authorized and must: 1) Identify the interface/connection. 2) Detail what data is involved and its sensitivity. 3) Determine whether the connection is one-way or bi-directional. 4) Identify how the connection is secured.
24	CA-5	None	Plan of Action and Milestones	Attest	Attestation - for compliance with FedRAMP Tailored LI-SaaS Continuous Monitoring Requirements
25	CA-6	None	Security Authorization	Document and Assess	
26	CA-7	None	Continuous Monitoring	Document and Assess	
27	CA-9	None	Internal System Connections	Document and Assess (Conditional)	Condition: There are connection(s) to external systems. Connections (if any) shall be authorized and must: 1) Identify the interface/connection. 2) Detail what data is involved and its sensitivity. 3) Determine whether the connection is one-way or bi-directional. 4) Identify how the connection is secured.
28	CM-1	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	Configuration Management Policy and Procedures	Attest	
29	CM-2	None	Baseline Configuration	Attest	
30	CM-4	A.14.2.3	Security Impact Analysis	Document and Assess	
31	CM-6	None	Configuration Settings	Document and Assess	
32	CM-7	A.12.5.1*	Least Functionality	Attest	
33	CM-8	A.8.1.1, A.8.1.2	Information System Component Inventory	Document and Assess	
34	CP-1	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	Contingency Planning Policy and Procedures	Attest	
35	CP-9	A.12.3.1, A.17.1.2, A.18.1.3	Information System Backup	Document and Assess	
36	IA-1	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	Identification and Authentication Policy and Procedures	Attest	
37	IA-2	A.9.2.1	Identification and Authentication (Organizational Users)	NSO, Attest	NSO - for non-privileged users. Attestation - for privileged users related to multi-factor identification and authentication. Include specific description of management of service accounts.

No	NIST 800-53 Control ID	ISO 27001 Control	NIST 800-53 Control Name	Tailoring Action	Additional Control Tailoring Comments
38	IA-2 (1)	A.9.2.1	Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts	Document and Assess	
39	IA-2 (12)	A.9.2.1	Identification and Authentication (Organizational Users) | Acceptance of Personal Identity Verification (PIV) Credentials	Document and Assess (Conditional)	Condition: Must document and assess for privileged users. May attest to this control for non-privileged users. FedRAMP requires a minimum of multi-factor authentication for all Federal privileged users, if acceptance of PIV credentials is not supported. The implementation status and details of how this control is implemented must be clearly defined by the CSP.
40	IA-4	A.9.2.1	Identifier Management	Attest	
41	IA-5	A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.3	Authenticator Management	Attest	
42	IA-5 (1)	A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.3	Authenticator Management | Password-Based Authentication	Attest	
43	IA-5 (11)	A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.3	Authenticator Management | Hardware Token-Based Authentication	FED, Document and Assess (Conditional)	FED - for Federal privileged users. Condition - Must document and assess for privileged users. May attest to this control for non-privileged users.
44	IA-6	A.9.4.2	Authenticator Feedback	Document and Assess	
45	IA-7	A.18.1.5	Cryptographic Module Authentication	Attest	
46	IA-8	A.9.2.1	Identification and Authentication (Non-Organizational Users)	Attest	
47	IA-8 (1)	A.9.2.1	Identification and Authentication (Non-Organizational Users) | Acceptance of PIV Credentials from Other Agencies	Document and Assess (Conditional)	Condition: Must document and assess for privileged users. May attest to this control for non-privileged users. FedRAMP requires a minimum of multi-factor authentication for all Federal privileged users, if acceptance of PIV credentials is not supported. The implementation status and details of how this control is implemented must be clearly defined by the CSP.
48	IA-8 (2)	A.9.2.1	Identification and Authentication (Non-Organizational Users) | Acceptance of Third-Party Credentials	Document and Assess (Conditional)	Condition: Must document and assess for privileged users. May attest to this control for non-privileged users. FedRAMP requires a minimum of multi-factor authentication for all Federal privileged users, if acceptance of PIV credentials is not supported. The implementation status and details of how this control is implemented must be clearly defined by the CSP.
49	IA-8 (3)	A.9.2.1	Identification and Authentication (Non-Organizational Users) | Acceptance of FICAM-Approved Products	Attest	

No	NIST 800-53 Control ID	ISO 27001 Control	NIST 800-53 Control Name	Tailoring Action	Additional Control Tailoring Comments
50	IA-8 (4)	A.9.2.1	Identification and Authentication (Non-Organizational Users) | Use of FICAM-Issued Profiles	Attest	
51	IR-1	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1 A.18.1.1, A.18.2.2	Incident Response Policy and Procedures	Attest	
52	IR-2	A.7.2.2*	Incident Response Training	Attest	
53	IR-4	A.16.1.4, A.16.1.5, A.16.1.6	Incident Handling	Document and Assess	
54	IR-5	None	Incident Monitoring	Attest	
55	IR-6	A.6.1.3, A.16.1.2	Incident Reporting	Document and Assess	
56	IR-7	None	Incident Response Assistance	Attest	
57	IR-8	A.16.1.1	Incident Response Plan	Attest	Attestation - Specifically attest to US-CERT compliance.
58	IR-9	None	Information Spillage Response	Attest	Attestation - Specifically describe information spillage response processes.
59	MA-1	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	System Maintenance Policy and Procedures	Attest	
60	MA-2	A.11.2.4*, A.11.2.5*	Controlled Maintenance	Document and Assess (Conditional)	Condition: Control is not inherited from a FedRAMP-authorized PaaS or IaaS.
61	MA-4	None	Non-local Maintenance	Attest	
62	MA-5	None	Maintenance Personnel	Document and Assess (Conditional)	Condition: Control is not inherited from a FedRAMP-authorized PaaS or IaaS.
63	MP-1	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	Media Protection Policy and Procedures	Attest	
64	MP-2	A.8.2.3, A.8.3.1, A.11.2.9	Media Access	Document and Assess (Conditional)	Condition: Control is not inherited from a FedRAMP-authorized PaaS or IaaS.
65	MP-6	A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7	Media Sanitization	Document and Assess (Conditional)	Condition: Control is not inherited from a FedRAMP-authorized PaaS or IaaS.
66	MP-7	A.8.2.3, A.8.3.1	Media Use	Document and Assess (Conditional)	Condition: Control is not inherited from a FedRAMP-authorized PaaS or IaaS.
67	PE-1	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	Physical and Environmental Protection Policy and Procedures	Attest	
68	PE-2	A.11.1.2*	Physical Access Authorizations	Document and Assess (Conditional)	Condition: Control is not inherited from a FedRAMP-authorized PaaS or IaaS.
69	PE-3	A.11.1.1, A.11.1.2, A.11.1.3	Physical Access Control	Document and Assess (Conditional)	Condition: Control is not inherited from a FedRAMP-authorized PaaS or IaaS.
70	PE-6	None	Monitoring Physical Access	Document and Assess (Conditional)	Condition: Control is not inherited from a FedRAMP-authorized PaaS or IaaS.

No	NIST 800-53 Control ID	ISO 27001 Control	NIST 800-53 Control Name	Tailoring Action	Additional Control Tailoring Comments
71	PE-8	None	Visitor Access Records	Document and Assess (Conditional)	Condition: Control is not inherited from a FedRAMP-authorized PaaS or IaaS.
72	PE-12	A.11.2.2*	Emergency Lighting	Document and Assess (Conditional)	Condition: Control is not inherited from a FedRAMP-authorized PaaS or IaaS.
73	PE-13	A.11.1.4, A.11.2.1	Fire Protection	Document and Assess (Conditional)	Condition: Control is not inherited from a FedRAMP-authorized PaaS or IaaS.
74	PE-14	A.11.1.4, A.11.2.1, A.11.2.2	Temperature and Humidity Controls	Document and Assess (Conditional)	Condition: Control is not inherited from a FedRAMP-authorized PaaS or IaaS.
75	PE-15	A.11.1.4, A.11.2.1, A.11.2.2	Water Damage Protection	Document and Assess (Conditional)	Condition: Control is not inherited from a FedRAMP-authorized PaaS or IaaS.
76	PE-16	A.8.2.3, A.11.1.6, A.11.2.5	Delivery and Removal	Document and Assess (Conditional)	Condition: Control is not inherited from a FedRAMP-authorized PaaS or IaaS.
77	PL-1	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	Security Planning Policy and Procedures	Attest	
78	PL-2	A.14.1.1	System Security Plan	Document and Assess	
79	PL-4	A.7.1.2, A.7.2.1, A.8.1.3	Rules of Behavior	Attest	
80	PS-1	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	Personnel Security Policy and Procedures	Attest	
81	PS-3	A.7.1.1	Personnel Screening	Document and Assess	
82	PS-4	A.7.3.1, A.8.1.4	Personnel Termination	Attest	
83	PS-5	A.7.3.1, A.8.1.4	Personnel Transfer	Attest	
84	PS-6	A.7.1.2, A.7.2.1, A.13.2.4	Access Agreements	Attest	
85	PS-7	A.6.1.1*, A.7.2.1*	Third-Party Personnel Security	Attest	Attestation - Specifically stating that any third-party security personnel are treated as CSP employees.
86	PS-8	A.7.2.3	Personnel Sanctions	Attest	
87	RA-1	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	Risk Assessment Policy and Procedures	Attest	
88	RA-2	A.8.2.1	Security Categorization	Document and Assess	
89	RA-3	A.12.6.1*	Risk Assessment	Document and Assess	
90	RA-5	A.12.6.1*	Vulnerability Scanning	Document and Assess	
91	SA-1	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	System and Services Acquisition Policy and Procedures	Attest	
92	SA-2	None	Allocation of Resources	Attest	

No	NIST 800-53 Control ID	ISO 27001 Control	NIST 800-53 Control Name	Tailoring Action	Additional Control Tailoring Comments
93	SA-3	A.6.1.1, A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.6	System Development Life Cycle	Attest	
94	SA-4	A.14.1.1, A.14.2.7, A.14.2.9, A.15.1.2	Acquisition Process	Attest	
95	SA-4 (10)	A.14.1.1, A.14.2.7, A.14.2.9, A.15.1.2	Acquisition Process | Use of Approved PIV Products	Attest	
96	SA-5	A.12.1.1*	Information System Documentation	Attest	
97	SA-9	A.6.1.1, A.6.1.5, A.7.2.1, A.13.1.2, A.13.2.2, A.15.2.1, A.15.2.2	External Information System Services	Document and Assess	
98	SC-1	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	System and Communications Protection Policy and Procedures	Attest	
99	SC-5	None	Denial of Service Protection	Document and Assess (Conditional)	Condition: If availability is a requirement - define protections in place as per control requirement .
100	SC-7	A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.3	Boundary Protection	Document and Assess	
101	SC-12	A.10.1.2	Cryptographic Key Establishment and Management	Document and Assess	
102	SC-13	A.10.1.1, A.14.1.2, A.14.1.3, A.18.1.5	Conditional Cryptographic Protection	Document and Assess (Conditional)	Condition: If implementing need to detail how they meet it or not.
103	SC-20	None	Secure Name /Address Resolution Service (Authoritative Source)	Attest	
104	SC-21	None	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	Attest	
105	SC-22	None	Architecture and Provisioning for Name/Address Resolution Service	Attest	
106	SC-39	None	Process Isolation	Attest	
107	SI-1	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	System and Information Integrity Policy and Procedures	Attest	
108	SI-2	A.12.6.1, A.14.2.2, A.14.2.3, A.16.1.3	Flaw Remediation	Document and Assess	
109	SI-3	A.12.2.1	Malicious Code Protection	Document and Assess	
110	SI-4	None	Information System Monitoring	Document and Assess	
111	SI-5	A.6.1.4*	Security Alerts, Advisories, and Directives	Attest	
112	SI-12	None	Information Handling and Retention	Attest	Attestation - Specifically related to US-CERT and FedRAMP communications procedures.