FedRAMP Control Quick Guide

Control requirements are identified in the FedRAMP SSP

ID	Family	Low	Moderate
AC	Access Control	11	18 (25)
AT	Awareness and Training	4	4 (1)
AU	Audit and Accountability	10	11 (8)
CA	Certification, Accreditation, and Security Assessment	7 (1)	8 (7)
CM	Configuration Management	8	11 (15)
CP	Contingency Planning	6	9 (15)
IA	Identification and Authentication	7 (8)	8 (19)
IR	Incident Response	7	9 (9)
MA	Maintenance	4	6 (5)
MP	Media Protection	4	7 (3)
PE	Physical and Environmental Protection	10	16 (4)
PL	Planning	3	4 (2)
PS	Personnel Security	8	8 (1)
RA	Risk Assessment	4	4 (6)
SA	System and Services Acquisition	6 (1)	9 (13)
SC	System and Communications Protection	10	20 (12)
SI	System and Information Integrity	6	12 (16)
	Totals (Controls and Enhancements):	125	325

Legend:

Count = # of controls (#of enhancements)
Impact Level: L = Low / M = Moderate
Enhancements: (#, #)
Additional FedRAMP Requirements = ★
FedRAMP Guidance = G

Note: Controls and Enhancements added by FedRAMP are in **Bold**.

Access Control (AC)

Control #	Control Name	Control Baseline Low	Control Baseline Moderate	Additional Req.
AC-1	Access Control Policy and Procedures	L	M	
AC-2	Account Management	L	M(1,2,3,4,**5**,**7**,**9**,**10**,**12**)	★ G
AC-3	Access Enforcement	L	M	
AC-4	Information Flow Enforcement		M(**21**)	
AC-5	Separation of Duties		M	G
AC-6	Least Privilege		M (1,2,5,9,10)	G
AC-7	Unsuccessful Logon Attempts	L	M	
AC-8	System Use Notification	L	M	★ G
AC-10	Concurrent Session Control		**M**	
AC-11	Session Lock		M (1)	
AC-12	Session Termination		M	
AC-14	Permitted Actions Without Identification or Authentication	L	M	
AC-17	Remote Access	L	M (1,2,3,4,**9**)	
AC-18	Wireless Access	L	M (1)	
AC-19	Access Control For Mobile Devices	L	M (5)	
AC-20	Use of External Information Systems	L	M (1,2)	
AC-21	Information Sharing		M	
AC-22	Publicly Accessible Content	L	M	

Awareness and Training (AT)

Control #	Control Name	Control Baseline Low	Control Baseline Moderate	Additional Req.
AT-1	Security Awareness and Training Policy and Procedures	L	M	
AT-2	Security Awareness	L	M(2)	
AT-3	Security Training	L	M	
AT-4	Security Training Records	L	M	

Audit and Accountability (AU)

Control #	Control Name	Control Baseline Low	Control Baseline Moderate	Additional Req.
AU-1	Audit and Accountability Policy and Procedures	L	M	
AU-2	Audit Events	L	M (3)	G
AU-3	Content of Audit Records	L	M (1)	★ G
AU-4	Audit Storage Capacity	L	M	
AU-5	Response to Audit Processing Failures	L	M	
AU-6	Audit Review, Analysis, and Reporting	L	M (1,3)	
AU-7	Audit Reduction and Report Generation		M (1)	
AU-8	Time Stamps	L	M (1)	★ G
AU-9	Protection of Audit Information	L	M (**2**,4)	
AU-11	Audit Record Retention	L	M	★
AU-12	Audit Generation	L	M	

Certification, Accreditation, & Sec. Assessment (CA)

Control #	Control Name	Control Baseline Low	Control Baseline Moderate	Additional Req.
CA-1	Security Assessment and Authorization Policies and Procedures	L	M	
CA-2	Security Assessments	L (**1**)	M (1,**2**,**3**)	★
CA-3	System Interconnections	L	M (**3**,5)	G
CA-5	Plan of Action and Milestones	L	M	★
CA-6	Security Authorization	L	M	G
CA-7	Continuous Monitoring	L	M (1)	★ G
CA-8	Penetration Testing		**M** (**1**)	
CA-9	Internal System Connections	L	M	

Configuration Management (CM)

Control #	Control Name	Control Baseline Low	Control Baseline Moderate	Additional Req.
CM-1	Configuration Management Policy and Procedures	L	M	
CM-2	Baseline Configuration	L	M (1,**2**,3,7)	
CM-3	Configuration Change Control		M	★ G
CM-4	Security Impact Analysis	L	M	
CM-5	Access Restrictions For Change		M (**1**,**3**,**5**)	G
CM-6	Configuration Settings	L	M (1)	★ G
CM-7	Least Functionality	L	M (1,2,**5**)	★ G
CM-8	Information System Component Inventory	L	M (1,3,5)	★
CM-9	Configuration Management Plan		M	
CM-10	Software Usage Restrictions	L	M (**1**)	
CM-11	User-Installed Software	L	M	

Contingency Planning (CP)

Control #	Control Name	Control Baseline Low	Control Baseline Moderate	Additional Req.
CP-1	Contingency Planning Policy and Procedures	L	M	
CP-2	Contingency Plan	L	M (1,**2**,3,8)	★
CP-3	Contingency Training	L	M	
CP-4	Contingency Plan Testing	L	M (1)	★
CP-6	Alternate Storage Site		M (1,3)	
CP-7	Alternate Processing Site		M (1,2,3)	★ G
CP-8	Telecommunications Services		M (1,2)	★
CP-9	Information System Backup	L	M (1,**3**)	★
CP-10	Information System Recovery and Reconstitution	L	M (2)	

Identification and Authentication (IA)

Control #	Control Name	Control Baseline Low	Control Baseline Moderate	Additional Req.
IA-1	Identification and Authentication Policy and Procedures	L	M	
IA-2	Identification and Authentication (Organizational Users)	L (1, 12)	M (1,2,3,**5**,8, 11,12)	G
IA-3	Device Identification and Authentication		M	
IA-4	Identifier Management	L	M (**4**)	★
IA-5	Authenticator Management	L (1, 11)	M (1,2,3,**4**,**6**,**7**,11)	G
IA-6	Authenticator Feedback	L	M	
IA-7	Cryptographic Module Authentication	L	M	
IA-8	Identification and Authentication (Non-Organizational Users)	L(1,2, 3,4)	M (1,2,3,4)	

FedRAMP Rev. 4 Baseline

Incident Response (IR)

Control #	Control Name	Control Baseline Low	Control Baseline Moderate	Additional Req.
IR-1	Incident Response Policy and Procedures	L	M	
IR-2	Incident Response Training	L	M	
IR-3	Incident Response Testing		M (2)	★
IR-4	Incident Handling	L	M (1)	★
IR-5	Incident Monitoring	L	M	
IR-6	Incident Reporting	L	M (1)	★
IR-7	Incident Response Assistance	L	M (1,**2**)	
IR-8	Incident Response Plan	L	M	★
IR-9	Information Spillage Response		**M** (**1**,**2**,**3**,**4**)	

Maintenance (MA)

Control #	Control Name	Control Baseline Low	Control Baseline Moderate	Additional Req.
MA-1	System Maintenance Policy and Procedures	L	M	
MA-2	Controlled Maintenance	L	M	
MA-3	Maintenance Tools		M (1,2,**3**)	
MA-4	Nonlocal Maintenance	L	M (2)	
MA-5	Maintenance Personnel	L	M (**1**)	★
MA-6	Timely Maintenance		M	

Media Protection (MP)

Control #	Control Name	Control Baseline Low	Control Baseline Moderate	Additional Req.
MP-1	Media Protection Policy and Procedures	L	M	
MP-2	Media Access	L	M	
MP-3	Media Marking		M	G
MP-4	Media Storage		M	★
MP-5	Media Transport		M (4)	★
MP-6	Media Sanitization	L	M (**2**)	G
MP-7	Media Use	L	M (1)	

Physical and Environmental Protection (PE)

Control #	Control Name	Control Baseline Low	Control Baseline Moderate	Additional Req.
PE-1	Physical and Environmental Protection Policy and Procedures	L	M	G
PE-2	Physical Access Authorizations	L	M	
PE-3	Physical Access Control	L	M	
PE-4	Access Control For Transmission Medium		M	
PE-5	Access Control For Output Devices		M	
PE-6	Monitoring Physical Access	L	M (1)	
PE-8	Visitor Access Records	L	M	
PE-9	Power Equipment and Cabling		M	
PE-10	Emergency Shutoff		M	
PE-11	Emergency Power		M	
PE-12	Emergency Lighting	L	M	
PE-13	Fire Protection	L	M (**2**,3)	
PE-14	Temperature and Humidity Controls	L	M (**2**)	★
PE-15	Water Damage Protection	L	M	
PE-16	Delivery and Removal	L	M	
PE-17	Alternate Work Site		M	

Planning (PL)

Control #	Control Name	Control Baseline Low	Control Baseline Moderate	Additional Req.
PL-1	Security Planning Policy and Procedures	L	M	
PL-2	System Security Plan	L	M (3)	
PL-4	Rules of Behavior	L	M (1)	
PL-8	Information Security Architecture		M	

Personnel Security (PS)

Control #	Control Name	Control Baseline Low	Control Baseline Moderate	Additional Req.
PS-1	Personnel Security Policy and Procedures	L	M	
PS-2	Position Risk Designation	L	M	
PS-3	Personnel Screening	L	M (**3**)	
PS-4	Personnel Termination	L	M	
PS-5	Personnel Transfer	L	M	
PS-6	Access Agreements	L	M	
PS-7	Third-Party Personnel Security	L	M	
PS-8	Personnel Sanctions	L	M	

Risk Assessment (RA)

Control #	Control Name	Control Baseline Low	Control Baseline Moderate	Additional Req.
RA-1	Risk Assessment Policy and Procedures	L	M	
RA-2	Security Categorization	L	M	
RA-3	Risk Assessment	L	M	★ G
RA-5	Vulnerability Scanning	L	M (1,2,3,**5**,**6**,**8**)	★ G

System and Services Acquisition (SA)

Control #	Control Name	Control Baseline Low	Control Baseline Moderate	Additional Req.
SA-1	System and Services Acquisition Policy and Procedures	L	M	
SA-2	Allocation of Resources	L	M	
SA-3	System Development Life Cycle	L	M	
SA-4	Acquisition Process	L (10)	M (1,2,**8**,9,10)	G
SA-5	Information System Documentation	L	M	
SA-8	Security Engineering Principles		M	
SA-9	External Information System Services	L	M (1,**2**,**4**,**5**)	★
SA-10	Developer Configuration Management		M (**1**)	★
SA-11	Developer Security Testing and Evaluation		M (**1**,**2**,**8**)	★

System and Communication Protection (SC)

Control #	Control Name	Control Baseline Low	Control Baseline Moderate	Additional Req.
SC-1	System and Communications Protection Policy and Procedures	L	M	
SC-2	Application Partitioning		M	
SC-4	Information In Shared Resources		M	
SC-5	Denial of Service Protection	L	M	
SC-6	Resource Availability		**M**	
SC-7	Boundary Protection	L	M (3,4,5,7, **8**, **12**,**13**,**18**)	★
SC-8	Transmission Confidentiality and Integrity		M (1)	
SC-10	Network Disconnect		M	G
SC-12	Cryptographic Key Establishment and Management	L	M (**2**,**3**)	★ G
SC-13	Cryptographic Protection	L	M	
SC-15	Collaborative Computing Devices	L	M	★
SC-17	Public Key Infrastructure Certificates		M	
SC-18	Mobile Code		M	
SC-19	Voice Over Internet Protocol		M	
SC-20	Secure Name / Address Resolution Service (Authoritative Source)	L	M	
SC-21	Secure Name / Address Resolution Service (Recursive or Caching Resolver)	L	M	
SC-22	Architecture and Provisioning for Name / Address Resolution Service	L	M	
SC-23	Session Authenticity		M	
SC-28	Protection of Information At Rest		M(**1**)	G
SC-39	Process Isolation	L	M	

System and Information Integrity (SI)

Control #	Control Name	Control Baseline Low	Control Baseline Moderate	Additional Req.
SI-1	System and Information Integrity Policy and Procedures	L	M	
SI-2	Flaw Remediation	L	M (2,**3**)	
SI-3	Malicious Code Protection	L	M (1,2,**7**)	
SI-4	Information System Monitoring	L	M (**1**,2,4,5,**14**,**16**, **23**)	G
SI-5	Security Alerts, Advisories, and Directives	L	M	★
SI-6	Security Function Verification		**M**	
SI-7	Software, Firmware, and Information Integrity		M (1,7)	
SI-8	Spam Protection		M (1,2)	
SI-10	Information Input Validation		M	
SI-11	Error Handling		M	
SI-12	Information Handling and Retention	L	M	
SI-16	Memory Protection		M	