FedRAMP Control Quick Guide

Control requirements are identified in the FedRAMP SSP

ID	Family	Class	Low Count	Moderate Count
AC	Access Control	Technical	11	17 (24)
AT	Awareness and Training	Operational	4	4
AU	Audit and Accountability	Technical	10	12 (9)
CA	Certification, Accreditation, and Security Assessment	Management	6 (1)	6 (2)
CM	Configuration Management	Operational	6	9 (12)
CP	Contingency Planning	Operational	6	9 (15)
IA	Identification and Authentication	Technical	7 (2)	8 (10)
IR	Incident Response	Operational	7	8 (4)
MA	Maintenance	Operational	4	6 (6)
MP	Media Protection	Operational	3	6 (5)
PE	Physical and Environmental Protection	Operational	11	18 (5)
PL	Planning	Management	4	5
PS	Personnel Security	Operational	8	8
RA	Risk Assessment	Management	4	4 (5)
SA	System and Services Acquisition	Management	8	12 (7)
SC	System and Communications Protection	Technical	8 (1)	24 (16)
SI	System and Information Integrity	Operational	5	12 (9)

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,**7**)	★
AC-3	Access Enforcement	L	M (**3**)	★
AC-4	Information Flow Enforcement		M	
AC-5	Separation of Duties		M	
AC-6	Least Privilege		M (1,2)	★ G
AC-7	Unsuccessful Login Attempts	L	M	
AC-8	System Use Notification	L	M	★ G
AC-10	**Concurrent Session Control**		**M**	
AC-11	Session Lock		M (**1**)	G
AC-14	Permitted Actions Without Identification/ Authentication	L	M (1)	
AC-16	**Security Attributes**		**M**	★
AC-17	Remote Access	L	M (1,2,3,4,5, 7,8)	★ G
AC-18	Wireless Access	L	M (1,**2**)	
AC-19	Access Control for Mobile Devices	L	M (1,2,3)	★
AC-20	Use of External Information Systems	L	M (1,2)	
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	
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	Auditable Events	L	M (3,4)	★ 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**)	
AU-10	**Non-Repudiation**		**M (5)**	★
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)	
CA-3	Information System Connections	L	M	
CA-5	Plan of Action and Milestones	L	M	
CA-6	Security Authorization	L	M	G
CA-7	Continuous Monitoring	L	M (**2**)	

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 (1,3,**5**)	★ G
CM-3	Configuration Change Control		M (2)	★
CM-4	Security Impact Analysis	L	M	
CM-5	Access Restrictions for Change		M (**1,5**)	
CM-6	Configuration Settings	L	M (1,3)	★ G
CM-7	Least Functionality	L	M (1)	★ G
CM-8	Information System Component Inventory	L	M (1,**3**,5)	★ G
CM-9	Configuration Management Plan		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**)	★
CP-3	Contingency Training	L	M	
CP-4	Contingency Plan Testing and Exercises	L	M (1)	★
CP-6	Alternate Storage Site		M (1,3)	
CP-7	Alternate Processing Site		M (1,2,3,5)	★
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 (2,3)	★

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)	M (1,2,3,8)	★
IA-3	Device Identification and Authentication		M	★
IA-4	Identifier Management	L	M (**4**)	★
IA-5	Authenticator Management	L (1)	M (1,2,3,**6,7**)	G
IA-6	Authenticator Feedback	L	M	
IA-7	Cryptographic Module Authentication	L	M	
IA-8	Identification and Authentication (Non-Organizational Users)	L	M	

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 and Exercises		M	★
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	★

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 (1)	
MA-3	Maintenance Tools		M (1,2,**3**)	
MA-4	Non-Local Maintenance	L	M (1,2)	
MA-5	Maintenance Personnel	L	M	
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 (1)	★
MP-3	Media Marking		M	
MP-4	Media Storage		M (**1**)	★
MP-5	Media Transport		M (2,4)	★
MP-6	Media Sanitization	L	M (**4**)	

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	
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-7	Visitor Control	L	M (1)	
PE-8	Access Records	L	M	
PE-9	Power Equipment and Power Cabling		M	
PE-10	Emergency Shutoff		M	★
PE-11	Emergency Power		M	
PE-12	Emergency Lighting	L	M	
PE-13	Fire Protection	L	M (1,2,3)	
PE-14	Temperature and Humidity Controls	L	M	★
PE-15	Water Damage Protection	L	M	
PE-16	Delivery and Removal	L	M	
PE-17	Alternate Work Site		M	★
PE-18	Location of Information System Components		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	
PL-4	Rules of Behavior	L	M	
PL-5	Privacy Impact Assessment	L	M	
PL-6	Security-Related Activity Planning		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 Categorization	L	M	
PS-3	Personnel Screening	L	M	
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,**2,3,5,6,9**)	★ 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	Life Cycle Support	L	M	
SA-4	Acquisitions	L	M (1,4,**7**)	G
SA-5	Information System Documentation	L	M (1,3)	
SA-6	Software Usage Restrictions	L	M	
SA-7	User-Installed Software	L	M	
SA-8	Security Engineering Principles		M	
SA-9	External Information System Services	L	M (**1**)	★
SA-10	Developer Configuration Management		M	
SA-11	Developer Security Testing		M (**1**)	★
SA-12	**Supply Chain Protection**		**M**	★

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 Priority**		**M**	
SC-7	Boundary Protection	L	M (1,2,3,4,5,7, **8, 12,13,18**)	★
SC-8	Transmission Integrity		M (1)	
SC-9	Transmission Confidentiality		M (1)	★
SC-10	Network Disconnect		M	G
SC-11	**Trusted Path**		M	★
SC-12	Cryptographic Key Establishment and Management	L	M (**2,5**)	★
SC-13	Use of Cryptography	L	M (**1**)	
SC-14	Public Access Protections	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 (1)	M (1)	
SC-21	**Secure Name/ Address Resolution Service (Recursive or Caching Resolver)**		**M**	
SC-22	Architecture and Provisioning for Name/ Address Resolution Service		M	
SC-23	Session Authenticity		M	
SC-28	Protection of Information at Rest		M	★
SC-30	**Virtualization Techniques**		**M**	
SC-32	Information System Partitioning		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)	
SI-3	Malicious Code Protection	L	M (1,2,3)	
SI-4	Information System Monitoring		M (2,4,5,6)	★ G
SI-5	Security Alerts, Advisories, and Directives	L	M	★
SI-6	**Security functionality verification**		**M**	
SI-7	Software and Information Integrity		M (1)	
SI-8	Spam Protection		M	
SI-9	Information Input Restrictions		M	
SI-10	Information Input Validation		M	
SI-11	Error Handling		M	
SI-12	Information Output Handling and Retention	L	M	