



FedRAMP Control Quick Reference Guide

Based on NIST SP 800-53 Revision 5
Control requirements as listed in the FedRAMP SSP

Control Requirements Summary

ID	Control Family	Moderate Count	High Count
AU	Audit and Accountability	16	27
SR	Supply Chain Risk Management	12	14
SI	System and Information Integrity	24	35
SA	System and Services Acquisition	20	24
SC	System and Communications Protection	29	35
PS	Personnel Security	10	11
PL	Planning	7	7
PE	Physical And Environmental Protection	19	26
MP	Media Protection	7	10
MA	Maintenance	10	12
AT	Awareness and Training	6	6
IR	Incident Response	17	24
IA	Identification and Authentication	27	30
CP	Contingency Planning	23	35
RA	Risk Assessment	11	13
CM	Configuration Management	27	34
AC	Access Control	43	50
CA	Assessment, Authorization, and Monitoring	14	16
Total Controls:		322	409

Legend: Impact Level: M = Moderate / H = High

Audit and Accountability

Control ID	Control Name	Control Baseline	
AU-1	Policy and Procedures	M	H
AU-2	Event Logging	M	H
AT-3	Content of Audit Records	M (1)	H (1)
AU-4	Audit Log Storage Capacity	M	H
AU-5	Response to Audit Logging Process Failures	M	H (1, 2)
AU-6	Audit Record Review, Analysis, and Reporting	M (1, 3)	H (1, 3, 4, 5, 6, 7)
AU-7	Audit Record Reduction and Report Generation	M (1)	H (1)
AU-8	Time Stamps	M	H
AU-9	Protection of Audit Information	M (4)	H (2, 3, 4)
AU-10	Non-repudiation		H
AU-11	Audit Record Retention	M	H
AU-12	Audit Record Generation	M	H (1, 3)
Total Controls		16	27

Supply Chain Risk Management

Control ID	Control Name	Control Baseline	
SR-1	Policy and Procedures	M	H
SR-2	Supply Chain Risk Management Plan	M (1)	H (1)
SR-3	Supply Chain Controls and Processes	M	H
SR-5	Acquisition Strategies, Tools, and Methods	M	H
SR-6	Supplier Assessments and Reviews	M	H
SR-8	Notification Agreements	M	H
SR-9	Tamper Resistance and Detection		H (1)
SR-10	Inspection of Systems or Components	M	H
SR-11	Component Authenticity	M (1, 2)	H (1, 2)
SR-12	Component Disposal	M	H
Total Controls		12	14

System and Information Integrity

Control ID	Control Name	Control Baseline	
SI-1	Policy and Procedures	M	H
SI-2	Flaw Remediation	M (2, 3)	H (2, 3)
SI-3	Malicious Code Protection	M	H
SI-4	System Monitoring	M (1, 2, 4, 5, 16, 18, 23)	H (1, 2, 4, 5, 10, 11, 12, 14, 16, 18, 19, 20, 22, 23)
SI-5	Security Alerts, Advisories, and Directives	M	H (1)
SI-6	Security and Privacy Function Verification	M	H
SI-7	Software, Firmware, and Information Integrity	M (1, 7)	H (1, 2, 5, 7, 15)
SI-8	Spam Protection	M (2)	H (2)
SI-10	Information Input Validation	M	H
SI-11	Error Handling	M	H
SI-12	Information Management and Retention	M	H
SI-16	Memory Protection	M	H
Total Controls		24	35

System and Services Acquisition

Control ID	Control Name	Control Baseline	
SA-1	Policy and Procedures	M	H
SA-2	Allocation of Resources	M	H
SA-3	System Development Life Cycle	M	H
SA-4	Acquisition Process	M (1, 2, 9, 10)	H (1, 2, 5, 9, 10)
SA-5	System Documentation	M	H
SA-8	Security and Privacy Engineering Principles	M	H
SA-9	External System Services	M (1, 2, 5)	H (1, 2, 5)
SA-10	Developer Configuration Management	M	H
SA-11	Developer Testing and Evaluation	M (1, 2)	H (1, 2)
SA-15	Development Process, Standards, and Tools	M	H
SA-16	Developer-provided Training		H
SA-17	Developer Security and Privacy Architecture and Design		H
SA-21	Developer Screening		H
SA-22	Unsupported System Components	M	H
Total Controls		20	24

System and Communications Protection

Control ID	Control Name	Control Baseline	
SC-1	Policy and Procedures	M	H
SC-2	Separation of System and User Functionality	M	H
SC-3	Security Function Isolation		H
SC-4	Information in Shared System Resources	M	H
SC-5	Denial-of-service Protection	M	H
SC-7	Boundary Protection	M (3, 4, 5, 7, 8, 12, 18)	H (3, 4, 5, 7, 8, 10, 12, 18, 20, 21)
SC-8	Transmission Confidentiality and Integrity	M (1)	H (1)
SC-10	Network Disconnect	M	H
SC-12	Cryptographic Key Establishment and Management	M	H (1)
SC-13	Cryptographic Protection	M	H
SC-15	Collaborative Computing Devices and Applications	M	H
SC-17	Public Key Infrastructure Certificates	M	H
SC-18	Mobile Code	M	H
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	M	H
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	M	H
SC-22	Architecture and Provisioning for Name/Address Resolution Service	M	H
SC-23	Session Authenticity	M	H
SC-24	Fail in Known State		H
SC-28	Protection of Information at Rest	M (1)	H (1)
SC-39	Process Isolation	M	H
SC-45	System Time Synchronization	M (1)	H (1)
Total Controls		29	35

Personnel Security

Control ID	Control Name	Control Baseline	
PS-1	Policy and Procedures	M	H
PS-2	Position Risk Designation	M	H
PS-3	Personnel Screening	M (3)	H (3)
PS-4	Personnel Termination	M	H (2)
PS-5	Personnel Transfer	M	H
PS-6	Access Agreements	M	H
PS-7	External Personnel Security	M	H
PS-8	Personnel Sanctions	M	H
PS-9	Position Descriptions	M	H
Total Controls		10	11

Planning

Control ID	Control Name	Control Baseline	
PL-1	Policy and Procedures	M	H
PL-2	System Security and Privacy Plans	M	H
PL-4	Rules of Behavior	M (1)	H (1)
PL-8	Security and Privacy Architectures	M	H
PL-10	Baseline Selection	M	H
PL-11	Baseline Tailoring	M	H
Total Controls		7	7

Physical And Environmental Protection			
Control ID	Control Name	Control Baseline	
PE-1	Policy and Procedures	M	H
PE-2	Physical Access Authorizations	M	H
PE-3	Physical Access Control	M	H (1)
PE-4	Access Control for Transmission	M	H
PE-5	Access Control for Output	M	H
PE-6	Monitoring Physical Access	M (1)	H (1, 4)
PE-8	Visitor Access Records	M	H (1)
PE-9	Power Equipment and Cabling	M	H
PE-10	Emergency Shutoff	M	H
PE-11	Emergency Power	M	H (1)
PE-12	Emergency Lighting	M	H
PE-13	Fire Protection	M (1, 2)	H (1, 2)
PE-14	Environmental Controls	M	H (2)
PE-15	Water Damage Protection	M	H (1)
PE-16	Delivery and Removal	M	H
PE-17	Alternate Work Site	M	H
PE-18	Location of System Components		H
Total Controls		19	26

Incident Response			
Control ID	Control Name	Control Baseline	
IR-1	Policy and Procedures	M	H
IR-2	Incident Response Training	M	H (1, 2)
IR-3	Incident Response Testing	M (2)	H (2)
IR-4	Incident Handling	M (1)	H (1, 2, 4, 6, 11)
IR-5	Incident Monitoring	M	H (1)
IR-6	Incident Reporting	M (1, 3)	H (1, 3)
IR-7	Incident Response Assistance	M (1)	H (1)
IR-8	Incident Response Plan	M	H
IR-9	Information Spillage Response	M (2, 3, 4)	H (2, 3, 4)
Total Controls		17	24

Configuration Management			
Control ID	Control Name	Control Baseline	
CM-1	Policy and Procedures	M	H
CM-2	Baseline Configuration	M (2, 3, 7)	H (2, 3, 7)
CM-3	Configuration Change Control	M (2, 4)	H (1, 2, 4, 6)
CM-4	Impact Analyses	M (2)	H (1, 2)
CM-5	Access Restrictions for Change	M (1, 5)	H (1, 5)
CM-6	Configuration Settings	M (1)	H (1, 2)
CM-7	Least Functionality	M (1, 2, 5)	H (1, 2, 5)
CM-8	System Component Inventory	M (1, 3)	H (1, 2, 3, 4)
CM-9	Configuration Management Plan	M	H
CM-10	Software Usage Restrictions	M	H
CM-11	User-installed Software	M	H
CM-12	Information Location	M (1)	H (1)
CM-14	Signed Components		H
Total Controls		27	34

Identification and Authentication			
Control ID	Control Name	Control Baseline	
IA-1	Policy and Procedures	M	H
IA-2	Identification and Authentication (Organizational Users)	M (1, 2, 5, 6, 8, 12)	H (1, 2, 5, 6, 8, 12)
IA-3	Device Identification and Authentication	M	H
IA-4	Identifier Management	M (4)	H (4)
IA-5	Authenticator Management	M (1, 2, 6, 7)	H (1, 2, 6, 7, 8, 13)
IA-6	Authentication Feedback	M	H
IA-7	Cryptographic Module Authentication	M	H
IA-8	Identification and Authentication (Non- Organizational Users)	M (1, 2, 4)	H (1, 2, 4)
IA-11	Re-authentication	M	H
IA-12	Identity Proofing	M (2, 3, 5)	H (2, 3, 4, 5)
Total Controls		27	30

Access Control			
Control ID	Control Name	Control Baseline	
AC-1	Access Control Policy and Procedures	M	H
AC-2	Account Management	M (1,2,3,4,5,7,9,12,13)	H (1,2,3,4,5,7,9,11,12,13)
AC-3	Access Enforcement		H
AC-4	Information Flow Enhancement	M (21)	H (4, 21)
AC-5	Separation of Duties	M	H
AC-6	Least Privilege	M (1, 2, 5, 7, 9, 10)	H (1, 2, 3, 5, 7, 8, 9, 10)
AC-7	Unsuccessful Logon Attempts	M	H
AC-8	System Use Notification	M	H
AC-10	Concurrent Session Control		H
AC-11	Device Lock	M (1)	H (1)
AC-12	Session Termination	M	H
AC-14	Permitted Actions Without Identification or Authentication	M	H
AC-17	Remote Access	M (1, 2, 3, 4)	H (1, 2, 3, 4)
AC-18	Wireless Access	M (1, 3)	H (1, 3, 4, 5)
AC-19	Access Control for Mobile Devices	M (5)	H (5)
AC-20	Use of External Systems	M (1, 2)	H (1, 2)
AC-21	Information Sharing	M	H
AC-22	Publicly Accessible Content	M	H
Total Controls		43	50

Media Protection			
Control ID	Control Name	Control Baseline	
MP-1	Policy and Procedures	M	H
MP-2	Media Access	M	H
MP-3	Media Marking	M	H
MP-4	Media Storage	M	H
MP-5	Media Transport	M	H
MP-6	Media Sanitization	M	H (1, 2, 3)
MP-7	Media Use	M	H
Total Controls		7	10

Contingency Planning			
Control ID	Control Name	Control Baseline	
CP-1	Policy and Procedures	M	H
CP-2	Contingency Plan	M (1, 3, 8)	H (1, 2, 3, 5, 8)
CP-3	Contingency Training	M	H (1)
CP-4	Contingency Plan Testing	M (1)	H (1, 2)
CP-6	Alternate Storage site	M (1, 3)	H (1, 2, 3)
CP-7	Alternate Processing Site	M (1, 2, 3)	H (1, 2, 3, 4)
CP-8	Telecommunications Services	M (1, 2)	H (1, 2, 3, 4)
CP-9	System Backup	M (1, 8)	H (1, 2, 3, 5, 8)
CP-10	System Recovery and Reconstitution	M (2)	H (2, 4)
Total Controls		23	35

Risk Assessment			
Control ID	Control Name	Control Baseline	
RA-1	Policy and Procedures	M	H
RA-2	Security Categorization	M	H
RA-3	Risk Assessment	M (1)	H (1)
RA-5	Vulnerability Monitoring and Scanning	M (2, 3, 5, 11)	H (2, 3, 4, 5, 8, 11)
RA-7	Risk Response	M	H
RA-9	Criticality Analysis	M	H
Total Controls		11	13

Assessment, Authorization, and Monitoring			
Control ID	Control Name	Control Baseline	
CA-1	Policy and Procedures	M	H
CA-2	Control Assessments	M (1, 3)	H (1, 2, 3)
CA-3	Information Exchange	M	H (6)
CA-5	Plan of Action and Milestones	M	H
CA-6	Authorization	M	H
CA-7	Continuous Monitoring	M (1, 4)	H (1, 4)
CA-8	Penetration Testing	M (1, 2)	H (1, 2)
CA-9	Internal System Connections	M	H
Total Controls		14	16

Awareness and Training			
Control ID	Control Name	Control Baseline	
AT-1	Awareness and Training Policy and Procedures	M	H
AT-2	Literacy Training and Awareness	M (2, 3)	H (2, 3)
AT-3	Role-based Training	M	H
AT-4	Training Records	M	H
Total Controls		6	6

Maintenance			
Control ID	Control Name	Control Baseline	
MA-1	Policy and Procedures	M	H
MA-2	Controlled Maintenance	M	H (2)
MA-3	Maintenance Tools	M (1, 2, 3)	H (1, 2, 3)
MA-4	Nonlocal Maintenance	M	H (3)
MA-5	Maintenance Personnel	M (1)	H (1)
MA-6	Timely Maintenance	M	H
Total Controls		10	12