September 30 2016
Version 3.1

FedRAMP Control

Quick Guide

Control requirements are identified in the FedRAMP SSP

ID	Control Description	Low	Moderate	High
AC	Access Control	11	43 (25)	54 (36)
AT	Awareness and Training	4	5 (1)	7 (3)
AU	Audit and Accountability	10	19 (8)	31 (19)
CA	Security Assessment and Authorization	8 (1)	15 (7)	16 (8)
CM	Configuration Management	8	26 (15)	36 (25)
CP	Contingency Planning	6	24 (15)	35 (26)
IA	Identification and Authentication	15 (8)	27 (19)	31 (23)
IR	Incident Response	7	18 (9)	26 (17)
MA	Maintenance	4	11 (5)	14 (8)
MP	Media Protection	4	10 (3)	12 (5)
PE	Physical and Environmental Protection	10	20 (4)	27 (10)
PL	Planning	3	6 (2)	6 (2)
PS	Personnel Security	8	9 (1)	10 (2)
RA	Risk Assessment	4	10 (6)	12 (8)
SA	System and Services Acquisition	6	22 (13)	26 (13)
SC	System and Communications Protection	10	32 (12)	39 (17)
SI	System and Information Integrity	7	28 (16)	39 (27)

Legend

0 (0)	Count = Total number of controls in each group (Total number of enhancements)
L	Impact Level: Low = L
M	Impact Level: Moderate or Mod = M
H	Impact Level: High = H
(0) (0)	Control enhancement identifier (1) (2) (3)
FP	FedRAMP Parameter(s)
FR	Additional FedRAMP Requirements
FG	FedRAMP Guidance

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

LMH Quick Control Guide

Access Control (AC)

Control	Control Name	Control Baseline			Additional Req.
		Low	Moderate	High	
AC-1	Access Control Policy and Procedures	L	M	H	**FP**
AC-2	Account Management	L	M (1) (2) (3) (4) **(5) (7) (9) (10) (12)**	H (1) (2) (3) (4) (5) **(7) (9)** (10) (11) (12) (13)	**FP; FR; FG**
AC-3	Access Enforcement	L	M	H	
AC-4	Information Flow Enforcement		M **(21)**	H **(8) (21)**	
AC-5	Separation of Duties		M	H	**FG**
AC-6	Least Privilege		M (1) (2) (5) (9) (10)	H (1) (2) (3) (5) **(7) (8)** (9) (10)	**FP; FG**
AC-7	Unsuccessful Logon Attempts	L	M	H **(2)**	**FP**
AC-8	System Use Notification	L	M	H	**FP; FR**
AC-10	Concurrent Session Control		**M**	H	**FP**
AC-11	Session Lock		M (1)	H (1)	**FP**
AC-12	Session Termination		M	H **(1)**	**FG**
AC-14	Permitted Actions Without Identification or Authentication	L	M	H	
AC-17	Remote Access	L	M (1) (2) (3) (4) **(9)**	H (1) (2) (3) (4) **(9)**	**FP**
AC-18	Wireless Access	L	M (1)	H (1) **(3)** (4) (5)	
AC-19	Access Control For Mobile Devices	L	M (5)	H (5)	
AC-20	Use of External Information Systems	L	M (1) (2)	H (1) (2)	
AC-21	Information Sharing		M	H	
AC-22	Publicly Accessible Content	L	M	H	**FP**

Awareness and Training (AT)

Control	Control Name	Control Baseline			Additional Req.
		Low	Moderate	High	
AT-1	Security Awareness and Training Policy and Procedures	L	M	H	**FP**
AT-2	Security Awareness Training	L	M (2)	H (2)	**FP**
AT-3	Role-Based Security Training	L	M	H **(3) (4)**	**FP**
AT-4	Security Training Records	L	M	H	**FP**

Audit and Accountability (AU)

Control	Control Name	Control Baseline			Additional Req.
		Low	Moderate	High	
AU-1	Audit and Accountability Policy and Procedures	L	M	H	**FP**
AU-2	Audit Events	L	M (3)	H (3)	**FP; FR; FG**
AU-3	Content of Audit Records	L	M (1)	H (1) (2)	**FP; FR**
AU-4	Audit Storage Capacity	L	M	H	
AU-5	Response to Audit Processing Failures	L	M	H (1) (2)	**FP**
AU-6	Audit Review, Analysis and Reporting	L	M (1) (3)	H (1) (3) **(4)** (5) (6) **(7) (10)**	**FP; FR**
AU-7	Audit Reduction and Report Generation		M (1)	H (1)	
AU-8	Time Stamps	L	M (1)	H (1)	**FP; FR**
AU-9	Protection of Audit Information	L	M **(2)** (4)	H (2) (3) (4)	**FP**
AU-10	Non-repudiation			H	
AU-11	Audit Record Retention	L	M	H	**FP; FR**
AU-12	Audit Generation	L	M	H (1) (3)	**FP**

Security Assessment and Authorization (CA)

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

LMH Quick Control Guide

Configuration Management (CM)

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

*FedRAMP does not include CM-7 (4) in the Moderate Baseline. The NIST supplemental guidance states that CM-7 (4) is not required if CM-7 (5) is implemented.

Contingency Planning (CP)

Control	Control Name	Control Baseline			Additional Req.
		Low	Moderate	High	
CP-1	Contingency Planning Policy and Procedures	L	M	H	**FR**
CP-2	Contingency Plan	L	M (1) **(2)** (3) (8)	H (1) (2) (3) (4) (5) (8)	**FP; FR**
CP-3	Contingency Training	L	M	H (1)	**FP**
CP-4	Contingency Plan Testing	L	M (1)	H (1) (2)	**FP; FR**
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	Information System Backup	L	M (1) **(3)**	H (1) (2) (3) (5)	**FP; FR**
CP-10	Information System Recovery and Reconstitution	L	M (2)	H (2) (4)	

Identification and Authentication (IA)

Control	Control Name	Control Baseline			Additional Req.
		Low	Moderate	High	
IA-1	Identification and Authentication Policy and Procedures	L	M	H	**FP**
IA-2	Identification and Authentication (Organizational Users)	L (1) (12)	M (1) (2) (3) **(5)** (8) (11) (12)	H (1) (2) (3) (4) **(5)** (8) (9) (11) (12)	**FP; FG**
IA-3	Device Identification and Authentication		M	H	
IA-4	Identifier Management	L	M **(4)**	H **(4)**	**FP; FR; FG**
IA-5	Authenticator Management	L (1) (11)	M (1) (2) (3) **(4) (6) (7)** (11)	H (1) (2) (3) **(4) (6) (7) (8)** (11) **(13)**	**FP; FR; FG**
IA-6	Authenticator Feedback	L	M	H	
IA-7	Cryptographic Module Authentication	L	M	H	
IA-8	Identification and Authentication (Non-Organizational Users)	L (1) (2) (3) (4)	M (1) (2) (3) (4)	H (1) (2) (3) (4)	

Incident Response (IR)

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

Maintenance (MA)

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

LMH Quick Control Guide

Media Protection (MP)

Control	Control Name	Control Baseline			Additional Req.
		Low	Moderate	High	
MP-1	Media Protection Policy and Procedures	L	M	H	**FP**
MP-2	Media Access	L	M	H	
MP-3	Media Marking		M	H	**FP; FG**
MP-4	Media Storage		M	H	**FP; FR**
MP-5	Media Transport		M (4)	H (4)	**FP; FR**
MP-6	Media Sanitization	L	M **(2)**	H (1) (2) (3)	**FP; FG**
MP-7	Media Use	L	M (1)	H (1)	

Physical and Environmental Protection (PE)

Control	Control Name	Control Baseline			Additional Req.
		Low	Moderate	High	
PE-1	Physical and Environmental Protection Policy and Procedures	L	M	H	**FP**
PE-2	Physical Access Authorizations	L	M	H	**FP**
PE-3	Physical Access Control	L	M	H (1)	**FP**
PE-4	Access Control for Transmission Medium		M	H	
PE-5	Access Control for Output Devices		M	H	
PE-6	Monitoring Physical Access	L	M (1)	H (1) (4)	**FP**
PE-8	Visitor Access Records	L	M	H (1)	**FP**
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	L	M	H	
PE-13	Fire Protection	L	M **(2)** (3)	H (1) (2) (3)	
PE-14	Temperature and Humidity Controls	L	M **(2)**	H **(2)**	**FP; FR**
PE-15	Water Damage Protection	L	M	H (1)	
PE-16	Delivery and Removal	L	M	H	**FP**
PE-17	Alternate Work Site		M	H	
PE-18	Location of Information System Components			H	

Planning (PL)

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

Personnel Security (PS)

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

Risk Assessment (RA)

Control	Control Name	Control Baseline			Additional Req.
		Low	Moderate	High	
RA-1	Risk Assessment Policy and Procedures	L	M	H	**FP**
RA-2	Security Categorization	L	M	H	
RA-3	Risk Assessment	L	M	H	**FP; FG**
RA-5	Vulnerability Scanning	L	M (1) (2) **(3)** (5) **(6) (8)**	H (1) (2) **(3)** (4) (5) **(6) (8) (10)**	**FP; FR;**

LMH Quick Control Guide

System and Services Acquisition (SA)

Control	Control Name	Control Baseline			Additional Req.
		Low	Moderate	High	
SA-1	System and Services Acquisition Policy and Procedures	L	M	H	**FP**
SA-2	Allocation of Resources	L	M	H	
SA-3	System Development Life Cycle	L	M	H	
SA-4	Acquisition Process	L	M (1) (2) **(8)** (9) (10)	H (1) (2) **(8)** (9) (10)	**FP; FG**
SA-5	Information System Documentation	L	M	H	
SA-8	Security Engineering Principles		M	H	
SA-9	External Information System Services	L	M **(1)** (2) **(4) (5)**	H **(1)** (2) **(4) (5)**	**FP**
SA-10	Developer Configuration Management		M **(1)**	H **(1)**	**FP; FR**
SA-11	Developer Security Testing and Evaluation		M **(1) (2) (8)**	H **(1) (2) (8)**	**FR**
SA-12	Supply Chain Protection			H	
SA-15	Development Process, Standards, and Tools			H	
SA-16	Developer-Provided Training			H	
SA-17	Developer Security Architecture and Design			H	

System and Communications Protection

Control	Control Name	Control Baseline			Additional Req.
		Low	Moderate	High	
SC-1	System and Communications Protection Policy and Procedures	L	M	H	**FP**
SC-2	Application Partitioning		M	H	
SC-3	Security Function Isolation			H	
SC-4	Information in Shared Resources		M	H	
SC-5	Denial of Service Protection	L	M	H	
SC-6	Resource Availability		**M**	**H**	
SC-7	Boundary Protection	L	M (3) (4) (5) (7) **(8) (12) (13) (18)**	H (3) (4) (5) (7) (8) **(10) (12) (13)** (18) **(20)** (21)	**FP; FR**
SC-8	Transmission Confidentiality and Integrity		M (1)	H (1)	**FP**
SC-10	Network Disconnect		M	H	**FP**
SC-12	Cryptographic Key Establishment and Management	L	M **(2) (3)**	H (1) **(2) (3)**	**FP; FG**
SC-13	Cryptographic Protection	L	M	H	**FP**
SC-15	Collaborative Computing Devices	L	M	H	**FP; FR**
SC-17	Public Key Infrastructure Certificates		M	H	
SC-18	Mobile Code		M	H	
SC-19	Voice Over Internet Protocol		M	H	
SC-20	Secure Name /Address Resolution Service (Authoritative Source	L	M	H	
SC-21	Secure Name /Address Resolution Service (Recursive or Caching	L	M	H	
SC-22	Architecture and Provisioning for Name/Address Resolution Ser	L	M	H	
SC-23	Session Authenticity		M	H **(1)**	
SC-24	Fail in Known State			H	
SC-28	Protection of Information at Rest		M **(1)**	H **(1)**	**FP; FG**
SC-39	Process Isolation	L	M	H	

System and Information Integrity (SI)

Control	Control Name	Control Baseline			Additional Req.
		Low	Moderate	High	
SI-1	System and Information Integrity Policy and Procedures	L	M	H	**FP**
SI-2	Flaw Remediation	L	M (2) **(3)**	H (1) (2) **(3)**	**FP**
SI-3	Malicious Code Protection	L	M (1) (2) **(7)**	H (1) (2) **(7)**	**FP**
SI-4	Information System Monitoring	L	M **(1)** (2) (4) (5) **(14) (16) (23)**	H **(1)** (2) (4) (5) **(11) (14) (16) (18) (19) (20) (22) (23) (24)**	**FP; FG**
SI-5	Security Alerts, Advisories, and Directives	L	M	H (1)	**FP**
SI-6	Security Function Verification		**M**	H	**FP**
SI-7	Software, Firmware, and Information Integrity		M (1) (7)	H (1) (2) (5) (7) (14)	**FP**
SI-8	Spam Protection		M (1) (2)	H (1) (2)	
SI-10	Information Input Validation		M	H	
SI-11	Error Handling		M	H	
SI-12	Information Handling and Retention	L	M	H	
SI-16	Memory Protection	L	M	H	