



Quick Control Guide - MODERATE Impact Controls

Access Control (AC)

Control	Control Name	Add'l Req.
AC-1	Access Control Policy and Procedures	FP
AC-2	Account Management (1) (2) (3) (4) (5) (7) (9) (10) (12)	FP; FR; FG
AC-3	Access Enforcement	
AC-4	Information Flow Enforcement (21)	
AC-5	Separation of Duties	FG
AC-6	Least Privilege (1) (2) (5) (9) (10)	FP; FG
AC-7	Unsuccessful Logon Attempts	FP
AC-8	System Use Notification	FP; FR
AC-10	Concurrent Session Control	FP
AC-11	Session Lock (1)	FP
AC-12	Session Termination	
AC-14	Permitted Actions Without Identification or Authentication	
AC-15	Withdrawn	
AC-16	Security Attributes	
AC-17	Remote Access (1) (2) (3) (4) (9)	FP
AC-18	Wireless Access (1)	
AC-19	Access Control For Mobile Devices (5)	
AC-20	Use of External Information Systems	
AC-21	Information Sharing (1) (2)	
AC-22	Publicly Accessible Content	FP

Awareness and Training (AT)

Control	Control Name	Add'l Req.
AT-1	Security Awareness and Training Policy and Procedures	FP
AT-2	Security Awareness Training (2)	FP
AT-3	Role-Based Security Training	FP
AT-4	Security Training Records	FP

Audit and Accountability (AU)

Control	Control Name	Add'l Req.
AU-1	Audit and Accountability Policy and Procedures	FP
AU-2	Audit Events (3)	FP; FR; FG
AU-3	Content of Audit Records (1)	FP; FR
AU-4	Audit Storage Capacity	
AU-5	Response to Audit Processing Failures	FP
AU-6	Audit Review, Analysis and Reporting (1) (3)	FP; FR
AU-7	Audit Reduction and Report Generation (1)	
AU-8	Time Stamps (1)	FP; FR
AU-9	Protection of Audit Information (2) (4)	FP
AU-11	Audit Record Retention	FP
AU-12	Audit Generation	FP; FR

Security Assessment and Authorization (CA)

Control	Control Name	Add'l Req.
CA-1	Security Assessment and Authorization Policies and Procedures	FP
CA-2	Security Assessments (1) (2) (3)	FP; FR
CA-3	System Interconnections (3) (5)	FP; FG
CA-5	Plan of Action and Milestones	FP; FG
CA-6	Security Authorization	FP; FG
CA-7	Continuous Monitoring (1)	FP; FR; FG
CA-8	Penetration Testing (1)	FP
CA-9	Internal System Connections	

KEY: **BOLD** = Controls and Enhancements added by FedRAMP
 (n) Enhancement number (e.g., (1), (2))
 FP = FedRAMP Parameter
 FR = Additional FedRAMP Requirements
 FG = FedRAMP Guidance

Configuration Management (CM)

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

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

Contingency Planning (CP)

Control	Control Name	Add'l Req.
CP-1	Contingency Planning Policy and Procedures	FP
CP-2	Contingency Plan Testing (1) (2) (3) (8)	FP; FR
CP-3	Contingency Training	FP
CP-4	Contingency Plan Testing (1)	FP; FR
CP-6	Alternate Storage Site (1) (3)	
CP-7	Alternate Processing Site (1) (2) (3)	FR; FG
CP-8	Telecommunications Services (1) (2)	FR
CP-9	Information System Backup (1) (3)	FP; FR
CP-10	Information System Recovery & Reconstitution (2)	

Identification and Authentication (IA)

Control	Control Name	Add'l Req.
IA-1	Identification and Authentication Policy and Procedures	FP
IA-2	Identification & Authentication (Org. Users) (1) (2) (3) (5) (8) (11) (12)	FP; FG
IA-3	Device Identification and Authentication	
IA-4	Identifier Management (4)	FP; FR; FG
IA-5	Authenticator Management 1) (2) (3) (4) (5) (6) (11)	FP; FG
IA-6	Authenticator Feedback	
IA-7	Cryptographic Module Authentication	
IA-8	Identification and Authentication (Non-Org. Users) (1) (2) (3) (4)	

Incident Response (IR)

Control	Control Name	Add'l Req.
IR-1	Incident Response Policy and Procedures	FP
IR-2	Incident Response Training	FP
IR-3	Incident Response Testing (2)	FP; FR
IR-4	Incident Handling (1)	FR
IR-5	Incident Monitoring	
IR-6	Incident Reporting (1)	FP; FR
IR-7	Incident Response Assistance (1) (2)	
IR-8	Incident Response Plan	FP; FR
IR-9	Information Spillage Response (1) (2) (3) (4)	

Maintenance (MA)

Control	Control Name	Add'l Req.
MA-1	System Maintenance Policy and Procedures	FP
MA-2	Controlled Maintenance	
MA-3	Maintenance Tools (1) (2) (3)	FP
MA-4	Nonlocal Maintenance (1) (2)	
MA-5	Maintenance Personnel (1)	FR
MA-6	Timely Maintenance	



Quick Control Guide - MODERATE Impact Controls

Media Protection (MP)

Control	Control Name	Add'l Req.
MP-1	Media Protection Policy and Procedures	FP
MP-2	Media Access	
MP-3	Media Marking	FP; FG
MP-4	Media Storage	FP; FR
MP-5	Media Transport (4)	FP; FR
MP-6	Media Sanitization (2)	FP; FG
MP-7	Media Use (1)	

Physical and Environmental Protection (PE)

Control	Control Name	Add'l Req.
PE-1	Physical and Environmental Protection Policy and Procedures	FP
PE-2	Physical Access Authorizations	FP
PE-3	Physical Access Control	FP
PE-4	Access Control for Transmission Medium	
PE-5	Access Control for Output Devices	
PE-6	Monitoring Physical Access (1)	FP
PE-8	Visitor Access Records	FP
PE-9	Power Equipment and Cabling	
PE-10	Emergency Shutoff	
PE-11	Emergency Power	
PE-12	Emergency Lighting	
PE-13	Fire Protection (2) (3)	
PE-14	Temperature and Humidity Controls (2)	FP; FR
PE-15	Water Damage Protection	
PE-16	Delivery and Removal	FP
PE-17	Alternate Work Site	
PE-18	Location of Information System Components	

Planning (PL)

Control	Control Name	Add'l Req.
PL-1	Security Planning Policy and Procedures	FP
PL-2	System Security Plan (3)	FP
PL-4	Rules of Behavior (1)	FP
PL-8	Information Security Architecture	FP; FG

Personnel Security (PS)

Control	Control Name	Add'l Req.
PS-1	Personnel Security Policy and Procedures	FP
PS-2	Position Risk Designation	FP
PS-3	Personnel Screening (3)	FP
PS-4	Personnel Termination	FP
PS-5	Personnel Transfer	FP
PS-6	Access Agreements	FP
PS-7	Third-Party Personnel Security	FP
PS-8	Personnel Sanctions	

Risk Assessment (RA)

Control	Control Name	Add'l Req.
RA-1	Risk Assessment Policy and Procedures	FP
RA-2	Security Categorization	
RA-3	Risk Assessment	FP; FG
RA-5	Vulnerability Scanning (1) (2) (3) (5) (6) (8)	FP; FR; FG

System and Services Acquisition (SA)

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

System and Communications Protection

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

System and Information Integrity (SI)

Control	Control Name	Add'l Req.
SI-1	System and Information Integrity Policy and Procedures	FP
SI-2	Flaw Remediation (2) (3)	FP
SI-3	Malicious Code Protection (1) (2) (7)	FP
SI-4	Information System Monitoring (1) (2) (4) (5) (14) (16) (23)	FP; FG
SI-5	Security Alerts, Advisories, and Directives	FP
SI-6	Security Function Verification	FP
SI-7	Software, Firmware, and Information Integrity (1) (7)	FP
SI-8	Spam Protection (1) (2)	
SI-10	Information Input Validation	
SI-11	Error Handling	
SI-12	Information Handling and Retention	
SI-16	Memory Protection	