



Quick Reference Guide V1.0
for the CMS Required Security
and Privacy Control Baselines
based on NIST SP 800-53 Rev.4

Access Control (AC)									
Control		Non-Cloud Baselines			FedRAMP/Cloud Baselines				
		Low	Mod	High	Low	Mod	High		
AC-1	Access Control Policy and Procedures†	●	●	●	●	●	●		
AC-2	Account Management	●	[1, 2, 3, 4]	[1, 2, 3, 4, 5, 11, 12, 13]	●	[1, 2, 3, 4, 5, 7, 9, 10, 12]	[1, 2, 3, 4, 5, 7, 9, 10, 11, 12, 13]		
AC-3	Access Enforcement	●	●	●	●	●	●		
AC-4	Information Flow Enforcement		●	●		[21]	[8, 21]		
AC-5	Separation of Duties			●			●		
AC-6	Least Privilege		[1, 2, 5, 9, 10]	[1, 2, 3, 5, 9, 10]		[1, 2, 5, 9, 10]	[1, 2, 3, 5, 7, 8, 9, 10]		
AC-7	Unsuccessful Logon Attempts	●	●	●	●	●	[2]		
AC-8	System Use Notification	●	●	●	●	●	●		
AC-10	Concurrent Session Control			●		●	●		
AC-11	Session Lock		[1]	[1]		[1]	[1]		
AC-12	Session Termination		●	●		●	[1]		
AC-14	Permitted Actions Without Identification or Authentication	●	●	●	●	●	●		
AC-17	Remote Access	[9]	[1, 2, 3, 4, 9]	[1, 2, 3, 4, 9]	●	[1, 2, 3, 4, 9]	[1, 2, 3, 4, 9]		
AC-18	Wireless Access	●	[1]	[1, 4, 5]	●	[1]	[1, 3, 4, 5]		
AC-19	Access Control for Mobile Devices	●	[5]	[5]	●	[5]	[5]		
AC-20	Use of External Information Systems†	●	[1, 2]	[1, 2]	●	[1, 2]	[1, 2]		
AC-21	Information Sharing		●	●		●	●		
AC-22	Publicly Accessible Content	●	●	●	●	●	●		
Non-Mandatory: AC-9, AC-16 Omitted: AC-13, AC-15, AC-23, AC-24, AC-25									

Awareness and Training (AT)								
Control		Non-Cloud Baselines			FedRAMP/Cloud Baselines			
		Low	Mod	High	Low	Mod	High	
AT-1	Security Awareness and Training Policy and Procedures†	●	●	●	●	●	●	
AT-2	Security Awareness Training†	●	[2]	[2]	●	[2]	[2]	
AT-3	Role-Based Security Training †	●	●	●	●	●	[3, 4]	
AT-4	Security Training Records†	●	●	●	●	●	●	
Omitted: AT-5								

Audit and Accountability (AU)							
Control		Non-Cloud Baselines			FedRAMP/Cloud Baselines		
		Low	Mod	High	Low	Mod	High
AU-1	Audit and Accountability Policy and Procedures†	●	●	●	●	●	●
AU-2	Audit Events	●	[3]	[3]	●	[3]	[3]
AU-3	Content of Audit Records	●	[1]	[1, 2]	●	[1]	[1, 2]
AU-4	Audit Storage Capacity	●	●	●	●	●	●
AU-5	Response to Audit Processing Failures	●	●	[1, 2]	●	●	[1, 2]
AU-6	Audit Review, Analysis, and Reporting	●	[1, 3]	[1, 3, 5, 6]	●	[1, 3]	[1, 3, 4, 5, 6, 7, 10]
AU-7	Audit Reduction and Report Generation		[1]	[1]		[1]	[1]
AU-8	Time Stamps	●	[1]	[1]	●	[1]	[1]
AU-9	Protection of Audit Information	●	[4]	[2, 3, 4]	●	[2, 4]	[2, 3, 4]
AU-10	Non-Repudiation			●			●
AU-11	Audit Record Retention	●	●	●	●	●	●
AU-12	Audit Generation	●	●	[1, 3]	●	●	[1, 3]
Non-Mandatory: AU-16 Omitted: AU-13, AU-14, AU-15							

CISO Contact Information

CMS Information Security and Privacy Group (ISPG)

<https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html>

Mailto: CISO@cms.hhs.gov

Security Assessment and Authorization (CA)									
Control		Non-Cloud Baselines			FedRAMP/Cloud Baselines				
		Low	Mod	High	Low	Mod	High		
CA-1	Security Assessment and Authorization Policies and Procedures †	●	●	●	●	●	●		
CA-2	Security Assessments	●	[1]	[1, 2, 3]	[1]	[1, 2, 3]	[1, 2, 3]		
CA-3	System Interconnections	●	[5]	[5]	●	[3, 5]	[3, 5]		
CA-5	Plan of Action and Milestones	●	●	●	●	●	●		
CA-6	Security Authorization	●	●	●	●	●	●		
CA-7	Continuous Monitoring	●	[1]	[1]	●	[1]	[1, 3]		
CA-8	Penetration Testing		▲	●	●	[1]	[1]		
CA-9	Internal System Connections	●	●	●	●	●	●		
Omitted: CA-4									

Configuration Management (CM)									
Control		Non-Cloud Baselines			FedRAMP/Cloud Baselines				
		Low	Mod	High	Low	Mod	High		
CM-1	Configuration Management Policy and Procedures †	●	●	●	●	●	●		
CM-2	Baseline Configuration	●	[1, 3, 7]	[1, 2, 3, 7]	●	[1, 2, 3, 7]	[1, 2, 3, 7]		
CM-3	Configuration Change Control		[2]	[1, 2]		●	[1, 2, 4, 6]		
CM-4	Security Impact Analysis	●	●	[1]	●	●	[1]		
CM-5	Access Restrictions for Change		●	[1, 2, 3]		[1, 3, 5]	[1, 2, 3, 5]		
CM-6	Configuration Settings	●	●	[1, 2]	●	[1]	[1, 2]		
CM-7	Least Functionality	●	[1, 2, 4]	[1, 2, 5]	●	[1, 2, 5]	[1, 2, 5]		
CM-8	Information System Component Inventory	●	[1, 3, 5]	[1, 2, 3, 4, 5]	●	[1, 3, 5]	[1, 2, 3, 4, 5]		
CM-9	Configuration Management Plan		●	●		●	●		
CM-10	Software Usage Restrictions	●	●	●	●	[1]	[1]		
CM-11	User-Installed Software	●	●	●	●	●	[1]		

Contingency Planning (CP)									
Control		Non-Cloud Baselines			FedRAMP/Cloud Baselines				
		Low	Mod	High	Low	Mod	High		
CP-1	Contingency Planning Policy and Procedures†	●	●	●	●	●	●		
CP-2	Contingency Plan	●	[1, 3, 8]	[1, 2, 3, 4, 5, 8]	●	[1, 2, 3, 8]	[1, 2, 3, 4, 5, 8]		
CP-3	Contingency Training	●	●	[1]	●	●	[1]		
CP-4	Contingency Plan Testing	●	[1]	[1, 2]	●	[1]	[1, 2]		
CP-6	Alternate Storage Site		[1, 3]	[1, 2, 3]		[1, 3]	[1, 2, 3]		
CP-7	Alternate Processing Site		[1, 2, 3]	[1, 2, 3, 4]		[1, 2, 3]	[1, 2, 3, 4]		
CP-8	Telecommunications Services		[1, 2]	[1, 2, 3, 4]		[1, 2]	[1, 2, 3, 4]		
CP-9	Information System Backup	●	[1]	[1, 2, 3, 5]	●	[1, 3]	[1, 2, 3, 5]		
CP-10	Information System Recovery and Reconstitution	●	[2]	[2, 4]	●	[2]	[2, 4]		
Omitted: CP-5, CP-11, CP-12, CP-13									

Identity and Authentication (IA)								
Control		Non-Cloud Baselines			FedRAMP/Cloud Baselines			
		Low	Mod	High	Low	Mod	High	
IA-1	Identification and Authentication Policy and Procedures†	●	●	●	●	●	●	
IA-2	Identification and Authentication (Organizational Users)	[1, 11, 12]	[1, 2, 3, 8, 11, 12]	[1, 2, 3, 4, 8, 9, 11, 12]	[1, 12]	[1, 2, 3, 5, 8, 11, 12]	[1, 2, 3, 4, 5, 8, 9, 11, 12]	
IA-3	Device Identification and Authentication		●	●		●	●	
IA-4	Identifier Management	●	●	●	●	[4]	[4]	
IA-5	Authenticator Management	[1, 11]	[1, 2, 3, 11]	[1, 2, 3, 11]	[1, 11]	[1, 2, 3, 4, 6, 7, 11]	[1, 2, 3, 4, 6, 7, 8, 11, 13]	
IA-6	Authenticator Feedback	●	●	●	●	●	●	
IA-7	Cryptographic Module Authentication	●	●	●	●	●	●	
IA-8	Identification and Authentication (Non-Organizational Users)	[1, 2, 3, 4]	[1, 2, 3, 4]	[1, 2, 3, 4]	[1, 2, 3, 4]	[1, 2, 3, 4]	[1, 2, 3, 4]	
Omitted: IA-9, IA-10, IA-11								

Incident Response (IR)								
Control		Non-Cloud Baselines			FedRAMP/Cloud Baselines			
		Low	Mod	High	Low	Mod	High	
IR-1	Incident Response Policy and Procedures†	●	●	●	●	●	●	
IR-2	Incident Response Training	●	●	[1, 2]	●	●		[1, 2]
IR-3	Incident Response Testing		[2]	[2]		[2]		[2]
IR-4	Incident Handling	●	[1]	[1, 4]	●	[1]		[1, 2, 3, 4, 6, 8]
IR-5	Incident Monitoring	●	●	[1]	●	●		[1]
IR-6	Incident Reporting	●	[1]	[1]	●	[1]		[1]
IR-7	Incident Response Assistance	●	[1]	[1]	●	[1, 2]		[1, 2]
IR-8	Incident Response Plan	●	●	●	●	●		●
IR-9	Information Spillage Response					[1, 2, 3, 4]		[1, 2, 3, 4]
Non-Mandatory: IR-10								

Maintenance (MA)									
Control		Non-Cloud Baselines			FedRAMP/Cloud Baselines				
		Low	Mod	High	Low	Mod	High		
MA-1	System Maintenance Policy and Procedures†	●	●	●	●	●	●		
MA-2	Controlled Maintenance	●	●	[2]	●	●	[2]		
MA-3	Maintenance Tools		[1, 2]	[1, 2, 3]		[1, 2, 3]	[1, 2, 3]		
MA-4	Nonlocal Maintenance	●	[1, 2]	[1, 2, 3]	●	[2]	[2, 3, 6]		
MA-5	Maintenance Personnel	●	●	[1]	●	[1]	[1]		
MA-6	Timely Maintenance		●	●		●	●		

Media Protection (MP)							
Control		Non-Cloud Baselines			FedRAMP/Cloud Baselines		
		Low	Mod	High	Low	Mod	High
MP-1	Media Protection Policy and Procedures†	●	●	●	●	●	●
MP-2	Media Access	●	●	●	●	●	●
MP-3	Media Marking		●	●		●	●
MP-4	Media Storage		●	●		●	●
MP-5	Media Transport		[4]	[4]		[4]	[4]
MP-6	Media Sanitization	●	●	[1, 2, 3]	●	[2]	[1, 2, 3]
MP-7	Media Use	●	[1]	[1]	●	[1]	[1]
MP-CMS- 1	Media Related Records	●	●	●			
Non-Mandatory: MP-8							

Physical and Environmental Protection (PE)							
Control		Non-Cloud Baselines			FedRAMP/Cloud Baselines		
		Low	Mod	High	Low	Mod	High
PE-1	Physical and Environmental Protection Policy and Procedures†	●	●	●	●	●	●
PE-2	Physical Access Authorizations	●	●	●	●	●	●
PE-3	Physical Access Control	●		[1]	●	●	[1]
PE-4	Access Control for Transmission Medium		●	●		●	●
PE-5	Access Control for Output Devices		●	●		●	●
PE-6	Monitoring Physical Access	●	[1]	[1, 4]	●	[1]	[1, 4]
PE-8	Visitor Access Records	●		[1]	●	●	[1]
PE-9	Power Equipment and Cabling		●	●		●	●
PE-10	Emergency Shutoff		●	●		●	●
PE-11	Emergency Power		●	[1]		●	[1]
PE-12	Emergency Lighting	●	●	●	●	●	●
PE-13	Fire Protection	●	[3]	[1, 2, 3]	●	[2, 3]	[1, 2, 3]
PE-14	Temperature and Humidity Controls	●	●	●		[2]	[2]
PE-15	Water Damage Protection	●		[1]	●	●	[1]
PE-16	Delivery and Removal	●	●	●	●	●	●
PE-17	Alternate Work Site		●	●		●	●
PE-18	Location of Information System Components			●			●
Omitted: PE-7, PE-19, PE-20							

Planning (PL)							
Control		Non-Cloud Baselines			FedRAMP/Cloud Baselines		
		Low	Mod	High	Low	Mod	High
PL-1	Security Planning Policy and Procedures†	●	●	●	●	●	●
PL-2	System Security Plan	●	[3]	[3]	●	[3]	[3]
PL-4	Rules of Behavior†	●	[1]	[1]	●	[1]	[1]
PL-8	Information Security Architecture		●	●		●	●
Omitted: PL-3, PL-5, PL-6, PL-7, PL-9							

Personnel Security (PS)							
Control		Non-Cloud Baselines			FedRAMP/Cloud Baselines		
		Low	Mod	High	Low	Mod	High
PS-1	Personnel Security Policy and Procedures†	●	●	●	●	●	●
PS-2	Position Risk Designation	●	●	●	●	●	●
PS-3	Personnel Screening	●	●	●	●	[3]	[3]
PS-4	Personnel Termination	●	●	[2]	●	●	[2]
PS-5	Personnel Transfer	●	●	●	●	●	●
PS-6	Access Agreements	●	●	●	●	●	●
PS-7	Third-Party Personnel Security	●	●	●	●	●	●
PS-8	Personnel Sanctions	●	●	●	●	●	●

Risk Assessment (RA)							
Control		Non-Cloud Baselines			FedRAMP/Cloud Baselines		
		Low	Mod	High	Low	Mod	High
RA-1	Risk Assessment Policy and Procedures†	●	●	●	●	●	●
RA-2	Security Categorization	●	●	●	●	●	●
RA-3	Risk Assessment	●	●	●	●	●	●
RA-5	Vulnerability Scanning	●	[1, 2, 5]	[1, 2, 4, 5]	●	[1, 2, 3, 5, 6, 8]	[1, 2, 3, 4, 5, 6, 8, 10]
Omitted: RA-4, RA-6							

System and Services Acquisition (SA)							
Control		Non-Cloud Baselines			FedRAMP/Cloud Baselines		
		Low	Mod	High	Low	Mod	High
SA-1	System and Services Acquisition Policy and Procedures†	●	●	●	●	●	●
SA-2	Allocation of Resources	●	●	●	●	●	●
SA-3	System Development Life Cycle	●	●	●	●	●	●
SA-4	Acquisition Process	[10]	[1, 2, 9, 10]	[1, 2, 9, 10]	●	[1, 2, 8, 9, 10]	[1, 2, 8, 9, 10]
SA-5	Information System Documentation	●	●	●	●	●	●
SA-8	Security Engineering Principles		●	●		●	●
SA-9	External Information System Services	●	[2]	[2]	●	[1, 2, 4, 5]	[1, 2, 4, 5]
SA-10	Developer Configuration Management†		●	●		[1]	[1]
SA-11	Developer Security Testing and Evaluation		●	●		[1, 2, 8]	[1, 2, 8]

System and Services Acquisition (SA)							
Control		Non-Cloud Baselines			FedRAMP/Cloud Baselines		
		Low	Mod	High	Low	Mod	High
SA-12	Supply Chain Protection			●			●
SA-15	Development Process, Standards, and Tools		[9]	[9]			●
SA-16	Developer-Provided Training			●			●
SA-17	Developer Security Architecture and Design			●			●
Non-Mandatory: SA-13, SA-21, SA-22 Omitted: SA-6, SA-7, SA-14, SA-18, SA-19, SA-20							

System and Communications Protections (SC)							
Control		Non-Cloud Baselines			FedRAMP/Cloud Baselines		
		Low	Mod	High	Low	Mod	High
SC-1	System and Communications Protection Policy and Procedures†	●	●	●	●	●	●
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]	[3, 4, 5, 7, 8, 18, 21]	●	[3, 4, 5, 7, 8, 12, 13, 18]	[3, 4, 5, 7, 8, 10, 12, 13, 18, 20, 21]
SC-8	Transmission Confidentiality and Integrity		[1]	[1]		[1]	[1]
SC-10	Network Disconnect		●	●		●	●
SC-12	Cryptographic Key Establishment and Management	●	●	[1]	●	[2, 3]	[1, 2, 3]
SC-13	Cryptographic Protection	●	●	●	●	●	●
SC-15	Collaborative Computing Devices	[1]	[1]	[1]	●	●	●
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		●	●		●	[1]
SC-24	Fail in Known State			●			●
SC-28	Protection of Information at Rest		●	●		[1]	[1]
SC-39	Process Isolation	●	●	●	●	●	●
SC-CMS-1	Electronic Mail†		●	●			
SC-CMS-2	Website Usage	●	●	●			
Non-Mandatory: SC-32 Omitted: SC-9, SC-11, SC-14, SC-16, SC-25, SC-26, SC-27, SC-29, SC-30, SC-31, SC-33, SC-34, SC-35, SC-36, SC-37, SC-38, SC-40, SC-41, SC-42, SC-43, SC-44							

System and Information Integrity (SI)							
Control		Non-Cloud Baselines			FedRAMP/Cloud Baselines		
		Low	Mod	High	Low	Mod	High
SI-1	System and Information Integrity Policy and Procedures†	●	●	●	●	●	●
SI-2	Flaw Remediation	●	[2]	[1, 2]	●	[2, 3]	[1, 2, 3]
SI-3	Malicious Code Protection	●	[1, 2]	[1, 2]	●	[1, 2, 7]	[1, 2, 7]
SI-4	Information System Monitoring	●	[2, 4, 5]	[2, 4, 5]	●	[1, 2, 4, 5, 14, 16, 23]	[1, 2, 4, 5, 11, 14, 16, 18, 19, 20, 22, 23, 24]
SI-5	Security Alerts, Advisories, & Directives	●	●	[1]	●	●	[1]
SI-6	Security Function Verification			●		●	●
SI-7	Software, Firmware, and Information Integrity		[1, 7]	[1, 2, 5, 7, 14]		[1, 7]	[1, 2, 5, 7, 14]
SI-8	Spam Protection†		[1, 2]	[1, 2]		[1, 2]	[1, 2]
SI-10	Information Input Validation		●	●		●	●
SI-11	Error Handling		●	●		●	●
SI-12	Information Handling and Retention	●	●	●	●	●	●
SI-16	Memory Protection		●	●	●	●	●
Omitted: SI-9, SI-13, SI-14, SI-15, SI-17							

Program Management (PM)							
Control		All Baselines					
		Low	Mod	High			
PM-1	Information Security Program Plan†	●	●	●			
PM-2	Senior Information Security Officer†	●	●	●			
PM-3	Information Security Resources	●	●	●			
PM-4	Plan of Action and Milestones Process†	●	●	●			
PM-5	Information System Inventory	●	●	●			
PM-6	Information Security Measures of Performance†	●	●	●			
PM-7	Enterprise Architecture†	●	●	●			
PM-8	Critical Infrastructure Plan	●	●	●			
PM-9	Risk Management Strategy	●	●	●			
PM-10	Security Authorization Process	●	●	●			
PM-11	Mission/Business Process Definition	●	●	●			
PM-12	Insider Threat Program	●	●	●			
PM-13	Information Security Workforce	●	●	●			
PM-14	Testing, Training, and Monitoring	●	●	●			
PM-15	Contacts with Security Groups and Associations	●	●	●			
PM-16	Threat Awareness Program	●	●	●			

APPENDIX J							
Privacy Controls for Moderate and High Systems processing, storing, or transmitting PII and PHI (Applicable enhancements are required)							

Authority and Purpose (AP)							
AP-CMS-1	Authority and Purpose Policy and Procedures (Non-Mandatory) †						
AP-1	Authority to Collect						
AP-2	Purpose Specification						

Accountability, Audit, and Risk Management (AR)							
AR-CMS-1	Accountability, Audit, and Risk Management Policy and Procedures (Non-Mandatory)†						
AR-1	Governance and Privacy Program †						
AR-2	Privacy Impact and Risk Assessment †						
AR-3	Privacy Requirements for Contractors and Service Providers †						
AR-4	Privacy Monitoring and Auditing †						
AR-5	Privacy Awareness and Training †						
AR-6	Privacy Reporting						
AR-7	Privacy-Enhenced System Design and Development						
AR-8	Accounting Disclosures						

Data Quality and Integrity (DI)							
DI-CMS-1	Data Quality and Integrity Policy and Procedures (Non-Mandatory) †						
DI-1	Data Quality						
DI-2	Data Integrity and Data Integrity Board						

Data Minimization and Retention (DM)							
DM-CMS-1	Data Minimization and Retention Policy and Procedures (Non-Mandatory) †						
DM-1	Minimization of Personally Identifiable Information						
DM-2	Data Retention and Disposal						
DM-3	Minimization of PII Used in Testing, Training, and Research						

Individual Participation and Redress (IP)							
IP-CMS-1	Individual Participation and Redress Policy and Procedures (Non-Mandatory) †						
IP-1	Consent						
IP-2	Individual Access						
IP-3	Redress						
IP-4	Complaint Management						

Security (SE)							
SE-CMS-1	Security Policy and Procedures (Non-Mandatory) †						
SE-1	Inventory of Personally Identifiable Information						
SE-2	Privacy Incident Response						

Transparency (TR)	
TR-CMS-1	Security Policy and Procedures (Non-Mandatory) †
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Acts Statements
TR-3	Dissemination of Privacy Program Information