All 110 controls on one page - in assessor priority order

Priority = the DoD Assessment Methodology point value (v1.2.1, Annex A) - the exact weights behind your SPRS score. A failed 5-point control costs five times the score of a 1-point control. Work red first, then amber, then slate.

5 POINTS 44 controls - won or lost here (* = partial credit) **3 POINTS** 14 controls **1 POINT** 51 controls **NO SCORE** 3.12.4 SSP gate

ACCESS CONTROL (22 controls / 54 pts)	3.1.1	3.1.2	3.1.12	3.1.13	3.1.16	3.1.17	3.1.18	3.1.5	3.1.19	3.1.3	3.1.4
	3.1.6	3.1.7	3.1.8	3.1.9	3.1.10	3.1.11	3.1.14	3.1.15	3.1.20	3.1.21	3.1.22
AWARENESS AND TRAINING (3 controls / 11 pts)	3.2.1	3.2.2	3.2.3								
AUDIT AND ACCOUNTABILITY (9 controls / 19 pts)	3.3.1	3.3.5	3.3.2	3.3.3	3.3.4	3.3.6	3.3.7	3.3.8	3.3.9		
CONFIGURATION MANAGEMENT (9 controls / 33 pts)	3.4.1	3.4.2	3.4.5	3.4.6	3.4.7	3.4.8	3.4.3	3.4.4	3.4.9		
IDENTIFICATION AND AUTHENTICATION (11 controls / 27 pts)	3.5.1	3.5.2	3.5.3*	3.5.10	3.5.4	3.5.5	3.5.6	3.5.7	3.5.8	3.5.9	3.5.11
INCIDENT RESPONSE (3 controls / 11 pts)	3.6.1	3.6.2	3.6.3								
MAINTENANCE (6 controls / 18 pts)	3.7.2	3.7.5	3.7.1	3.7.4	3.7.3	3.7.6					
MEDIA PROTECTION (9 controls / 23 pts)	3.8.3	3.8.7	3.8.1	3.8.2	3.8.8	3.8.4	3.8.5	3.8.6	3.8.9		
PERSONNEL SECURITY (2 controls / 8 pts)	3.9.2	3.9.1									
PHYSICAL PROTECTION (6 controls / 14 pts)	3.10.1	3.10.2	3.10.3	3.10.4	3.10.5	3.10.6					
RISK ASSESSMENT (3 controls / 9 pts)	3.11.2	3.11.1	3.11.3								
SECURITY ASSESSMENT (4 controls / 13 pts)	3.12.1	3.12.3	3.12.2	3.12.4							
SYSTEM AND COMMUNICATIONS PROTECTION (16 controls / 42 pts)	3.13.1	3.13.2	3.13.5	3.13.6	3.13.11*	3.13.15	3.13.8	3.13.3	3.13.4	3.13.7	3.13.9
	3.13.10	3.13.12	3.13.13	3.13.14	3.13.16						
SYSTEM AND INFORMATION INTEGRITY (7 controls / 31 pts)	3.14.1	3.14.2	3.14.3	3.14.4	3.14.6	3.14.5	3.14.7				

** Partial credit built in: 3.5.3 (MFA) scores -3 if only remote/privileged users are covered, -5 if none. 3.13.11 (FIPS) scores -3 if encryption is not FIPS-validated, -5 if absent. Blue = 3.12.4 (SSP): no point value - without a System Security Plan the assessment cannot be conducted at all.*

The 44 five-point controls - where assessments are won or lost

DoD's methodology subtracts 5 points when a control's absence could enable significant exploitation of the network or exfiltration of CUI. These 44 controls carry 220 of the 313 deductible points. If your remediation plan doesn't start here, it starts in the wrong place.

ID	Family	Requirement
3.1.1	Access Control	Limit system access to authorized users, processes acting on behalf of authorized users, and devices
3.1.2	Access Control	Limit system access to the types of transactions and functions that authorized users are permitted ...
3.1.12	Access Control	Monitor and control remote access sessions
3.1.13	Access Control	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions
3.1.16	Access Control	Authorize wireless access prior to allowing such connections
3.1.17	Access Control	Protect wireless access using authentication and encryption
3.1.18	Access Control	Control connection of mobile devices
3.2.1	Awareness & Training	Ensure that managers, systems administrators, and users of organizational systems are made aware of ...
3.2.2	Awareness & Training	Ensure that personnel are trained to carry out their assigned information security-related duties ...
3.3.1	Audit & Accountability	Create and retain system audit logs and records to the extent needed to enable the monitoring, ...
3.3.5	Audit & Accountability	Correlate audit record review, analysis, and reporting processes for investigation and response to ...
3.4.1	Configuration Management	Establish and maintain baseline configurations and inventories of organizational systems (including ...
3.4.2	Configuration Management	Establish and enforce security configuration settings for information technology products employed ...
3.4.5	Configuration Management	Define, document, approve, and enforce physical and logical access restrictions associated with ...
3.4.6	Configuration Management	Employ the principle of least functionality by configuring organizational systems to provide only ...
3.4.7	Configuration Management	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and ...
3.4.8	Configuration Management	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or ...
3.5.1	Identification & Authentication	Identify system users, processes acting on behalf of users, and devices
3.5.2	Identification & Authentication	Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to ...
3.5.3*	Identification & Authentication	Use multifactor authentication for local and network access to privileged accounts and for network ...
3.5.10	Identification & Authentication	Store and transmit only cryptographically-protected passwords
3.6.1	Incident Response	Establish an operational incident-handling capability for organizational systems that includes ...
3.6.2	Incident Response	Track, document, and report incidents to designated officials and/or authorities both internal and ...
3.7.2	Maintenance	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system ...
3.7.5	Maintenance	Require multifactor authentication to establish nonlocal maintenance sessions via external network ...
3.8.3	Media Protection	Sanitize or destroy system media containing CUI before disposal or release for reuse
3.8.7	Media Protection	Control the use of removable media on system components
3.9.2	Personnel Security	Ensure that organizational systems containing CUI are protected during and after personnel actions ...
3.10.1	Physical Protection	Limit physical access to organizational systems, equipment, and the respective operating ...
3.10.2	Physical Protection	Protect and monitor the physical facility and support infrastructure for organizational systems
3.11.2	Risk Assessment	Scan for vulnerabilities in organizational systems and applications periodically and when new ...
3.12.1	Security Assessment	Periodically assess the security controls in organizational systems to determine if the controls ...
3.12.3	Security Assessment	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls
3.13.1	System & Comms Protection	Monitor, control, and protect communications at the external boundaries and key internal boundaries ...
3.13.2	System & Comms Protection	Employ architectural designs, software development techniques, and systems engineering principles ...
3.13.5	System & Comms Protection	Implement subnetworks for publicly accessible system components that are physically or logically ...
3.13.6	System & Comms Protection	Deny network communications traffic by default and allow network communications traffic by ...
3.13.11*	System & Comms Protection	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI
3.13.15	System & Comms Protection	Protect the authenticity of communications sessions
3.14.1	System & Info Integrity	Identify, report, and correct system flaws in a timely manner
3.14.2	System & Info Integrity	Provide protection from malicious code at designated locations within organizational systems
3.14.3	System & Info Integrity	Monitor system security alerts and advisories and take action in response
3.14.4	System & Info Integrity	Update malicious code protection mechanisms when new releases are available
3.14.6	System & Info Integrity	Monitor organizational systems, including inbound and outbound communications traffic, to detect ...

** Partial credit built into the methodology: 3.5.3 scores -3 if MFA covers only remote and privileged users; 3.13.11 scores -3 if encryption is employed but not FIPS-validated.*

How to use this map (as of mid-2026)

The CMMC Phase 2 rollout - third-party certification as a condition of award - was suspended by Department of War memo on July 13, 2026, pending a 60-day reform review. What did NOT change: DFARS 252.204-7012, NIST SP 800-171 implementation, SPRS score submission, and annual affirmations all remain contractually binding, and both underlying regulations remain in the CFR unamended. The deadline moved; the obligation didn't.

One thing got sharper: with third-party verification paused, your SPRS score is an unverified self-representation to the government - and the Department of Justice's Civil Cyber-Fraud Initiative treats false cybersecurity self-attestations as False Claims Act material. Score accuracy now matters more than certification timing.

The five-step triage

1. System Security Plan first (3.12.4).
No point value - because without it the assessment cannot happen at all. If your SSP is missing or stale, nothing else on this map counts yet.

2. Score yourself honestly against the 44 red controls.
They carry 220 of the 313 deductible points on a scoring range that runs from +110 down to -203. Most scores are decided here.

3. Check the two partial-credit traps.
MFA (3.5.3): remote + privileged users covered = -3 instead of -5. FIPS (3.13.11): encryption present but not FIPS-validated = -3 instead of -5. These are the two most commonly misplaced scores in self-assessments.

4. Clear the 14 amber controls.
Media protection, maintenance, and awareness controls that assessors treat as hygiene signals - cheap to fix, disproportionately visible.

5. Sweep the 51 slate controls last.
One point each. Necessary for a clean 110, but never the reason a contract is lost.

The SPRS math at a glance

Line item	Points
Starting score (all 110 requirements met)	**110**
Each unmet 5-point requirement (44 of them)	**-5**
Each unmet 3-point requirement (14 of them)	**-3**
Each unmet 1-point requirement (51 of them)	**-1**
MFA partial: remote + privileged users only (3.5.3)	**-3**
FIPS partial: encryption present, not FIPS-validated (3.13.11)	**-3**
No System Security Plan (3.12.4)	**no assessment**
Lowest possible score	**-203**

Your Basic Assessment score, its date, and the date you expect to reach 110 (your POA&M completion date) all go into SPRS - and primes increasingly check it before adding you to a team. A score you can defend line-by-line is worth more than a high one you can't.

Want your per-family score in three minutes?

Our free scored CMMC readiness assessment maps your posture across all 14 families and flags your gaps - no signup required: cabrilloclub.com/cmmc-assessment. Estimate certification cost with DoD's own figures: cabrilloclub.com/insights/tools/cmmc-cost

Source for all point values: NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1 (June 24, 2020), Annex A and Section 5 - the same weights used in SPRS scoring. Regulatory status as of July 2026. This document is general information, not legal or assessment advice.