CMMC SCORE ESTIMATOR · OCTOBER 2026

What's your SPRS score? All 110 NIST SP 800-171 requirements.

Mark each requirement met, not met or unsure — unsure counts as not met. Start at 110 and subtract the points for every requirement not met or unsure, using the DoD Assessment Methodology's 5-, 3- and 1-point weights. Total your estimate on the last page.

01
Mark
Go through the 110 NIST SP 800-171 requirements and mark each one met, not met or unsure (unsure counts as not met).

02
Score
Once all 110 are marked, you get your estimated SPRS score, using the DoD's 5-, 3- and 1-point weights.

03
Plan
See your biggest gaps, whether a POA&M could cover them, and print the list for your team.

COMPANY _____ DATE _____

COMPLETED BY _____ REVIEWED WITH _____

866.24.CALIT info@calitgroup.com calitgroup.com/cmmc-score-estimator

01 Access Control

Who can get into your systems and CUI, and what they can do once inside.

REQ.	REQUIREMENT	POINTS	STATUS
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.1.3	Control the flow of CUI in accordance with approved authorizations.	1	☐ Met ☐ Not met ☐ Unsure
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	1	☐ Met ☐ Not met ☐ Unsure
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts. Can't go on a POA&M for Conditional Level 2	3	☐ Met ☐ Not met ☐ Unsure
3.1.6	Use non-privileged accounts or roles when accessing non-security functions.	1	☐ Met ☐ Not met ☐ Unsure
3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	1	☐ Met ☐ Not met ☐ Unsure
3.1.8	Limit unsuccessful logon attempts.	1	☐ Met ☐ Not met ☐ Unsure
3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	1	☐ Met ☐ Not met ☐ Unsure
3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	1	☐ Met ☐ Not met ☐ Unsure
3.1.11	Terminate (automatically) a user session after a defined condition.	1	☐ Met ☐ Not met ☐ Unsure
3.1.12	Monitor and control remote access sessions. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.1.14	Route remote access via managed access control points.	1	☐ Met ☐ Not met ☐ Unsure
3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	1	☐ Met ☐ Not met ☐ Unsure
3.1.16	Authorize wireless access prior to allowing such connections. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.1.17	Protect wireless access using authentication and encryption. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.1.18	Control connection of mobile devices. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.1.19	Encrypt CUI on mobile devices and mobile computing platforms. Can't go on a POA&M for Conditional Level 2	3	☐ Met ☐ Not met ☐ Unsure
3.1.20	Verify and control/limit connections to and use of external systems. Can't go on a POA&M for Conditional Level 2	1	☐ Met ☐ Not met ☐ Unsure
3.1.21	Limit use of portable storage devices on external systems.	1	☐ Met ☐ Not met ☐ Unsure

REQ.	REQUIREMENT	POINTS	STATUS
3.1.22	Control CUI posted or processed on publicly accessible systems. Can't go on a POA&M for Conditional Level 2	1	☐ Met ☐ Not met ☐ Unsure

02 Awareness and Training

Making sure everyone knows the risks and their security duties.

REQ.	REQUIREMENT	POINTS	STATUS
3.2.1	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.2.2	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	1	☐ Met ☐ Not met ☐ Unsure

03 Audit and Accountability

Logging activity so you can trace what happened and who did it.

REQ.	REQUIREMENT	POINTS	STATUS
3.3.1	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. Can't go on a POA&M for Conditional Level 2	3	☐ Met ☐ Not met ☐ Unsure
3.3.3	Review and update logged events.	1	☐ Met ☐ Not met ☐ Unsure
3.3.4	Alert in the event of an audit logging process failure.	1	☐ Met ☐ Not met ☐ Unsure
3.3.5	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.3.6	Provide audit record reduction and report generation to support on-demand analysis and reporting.	1	☐ Met ☐ Not met ☐ Unsure
3.3.7	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	1	☐ Met ☐ Not met ☐ Unsure
3.3.8	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	1	☐ Met ☐ Not met ☐ Unsure
3.3.9	Limit management of audit logging functionality to a subset of privileged users.	1	☐ Met ☐ Not met ☐ Unsure

04 Configuration Management

Secure, documented settings and control over changes and software.

REQ.	REQUIREMENT	POINTS	STATUS
3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational systems. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.4.3	Track, review, approve or disapprove, and log changes to organizational systems.	1	☐ Met ☐ Not met ☐ Unsure
3.4.4	Analyze the security impact of changes prior to implementation.	1	☐ Met ☐ Not met ☐ Unsure
3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.4.8	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.4.9	Control and monitor user-installed software.	1	☐ Met ☐ Not met ☐ Unsure

05 Identification and Authentication

Unique accounts, strong passwords and multifactor authentication.

REQ.	REQUIREMENT	POINTS	STATUS
3.5.1	Identify system users, processes acting on behalf of users, and devices. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.5.2	Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. Can't go on a POA&M for Conditional Level 2 Partial credit: −3 instead of −5	5	☐ Met ☐ Not met ☐ Unsure
3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	1	☐ Met ☐ Not met ☐ Unsure
3.5.5	Prevent reuse of identifiers for a defined period.	1	☐ Met ☐ Not met ☐ Unsure
3.5.6	Disable identifiers after a defined period of inactivity.	1	☐ Met ☐ Not met ☐ Unsure

REQ.	REQUIREMENT	POINTS	STATUS
3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	1	☐ Met ☐ Not met ☐ Unsure
3.5.8	Prohibit password reuse for a specified number of generations.	1	☐ Met ☐ Not met ☐ Unsure
3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.	1	☐ Met ☐ Not met ☐ Unsure
3.5.10	Store and transmit only cryptographically-protected passwords. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.5.11	Obscure feedback of authentication information.	1	☐ Met ☐ Not met ☐ Unsure

06 Incident Response

Detecting, reporting and handling security incidents.

REQ.	REQUIREMENT	POINTS	STATUS
3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.6.2	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.6.3	Test the organizational incident response capability.	1	☐ Met ☐ Not met ☐ Unsure

07 Maintenance

Controlling who maintains your systems, and how.

REQ.	REQUIREMENT	POINTS	STATUS
3.7.1	Perform maintenance on organizational systems. Can't go on a POA&M for Conditional Level 2	3	☐ Met ☐ Not met ☐ Unsure
3.7.2	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	1	☐ Met ☐ Not met ☐ Unsure
3.7.4	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems. Can't go on a POA&M for Conditional Level 2	3	☐ Met ☐ Not met ☐ Unsure
3.7.5	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.7.6	Supervise the maintenance activities of maintenance personnel without required access authorization.	1	☐ Met ☐ Not met ☐ Unsure

08 Media Protection

Protecting, marking and destroying drives, USB sticks and paper that hold CUI.

REQ.	REQUIREMENT	POINTS	STATUS
3.8.1	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. Can't go on a POA&M for Conditional Level 2	3	☐ Met ☐ Not met ☐ Unsure
3.8.2	Limit access to CUI on system media to authorized users. Can't go on a POA&M for Conditional Level 2	3	☐ Met ☐ Not met ☐ Unsure
3.8.3	Sanitize or destroy system media containing CUI before disposal or release for reuse. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.8.4	Mark media with necessary CUI markings and distribution limitations.	1	☐ Met ☐ Not met ☐ Unsure
3.8.5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	1	☐ Met ☐ Not met ☐ Unsure
3.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	1	☐ Met ☐ Not met ☐ Unsure
3.8.7	Control the use of removable media on system components. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner. Can't go on a POA&M for Conditional Level 2	3	☐ Met ☐ Not met ☐ Unsure
3.8.9	Protect the confidentiality of backup CUI at storage locations.	1	☐ Met ☐ Not met ☐ Unsure

09 Personnel Security

Screening people before they get access, and removing it when they leave.

REQ.	REQUIREMENT	POINTS	STATUS
3.9.1	Screen individuals prior to authorizing access to organizational systems containing CUI. Can't go on a POA&M for Conditional Level 2	3	☐ Met ☐ Not met ☐ Unsure
3.9.2	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure

10 Physical Protection

Securing offices, visitors and equipment that hold CUI.

REQ.	REQUIREMENT	POINTS	STATUS
3.10.1	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure

REQ.	REQUIREMENT	POINTS	STATUS
3.10.2	Protect and monitor the physical facility and support infrastructure for organizational systems. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.10.3	Escort visitors and monitor visitor activity. Can't go on a POA&M for Conditional Level 2	1	☐ Met ☐ Not met ☐ Unsure
3.10.4	Maintain audit logs of physical access. Can't go on a POA&M for Conditional Level 2	1	☐ Met ☐ Not met ☐ Unsure
3.10.5	Control and manage physical access devices. Can't go on a POA&M for Conditional Level 2	1	☐ Met ☐ Not met ☐ Unsure
3.10.6	Enforce safeguarding measures for CUI at alternate work sites.	1	☐ Met ☐ Not met ☐ Unsure

11 Risk Assessment

Assessing risk regularly and scanning for vulnerabilities.

REQ.	REQUIREMENT	POINTS	STATUS
3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. Can't go on a POA&M for Conditional Level 2	3	☐ Met ☐ Not met ☐ Unsure
3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.11.3	Remediate vulnerabilities in accordance with risk assessments.	1	☐ Met ☐ Not met ☐ Unsure

12 Security Assessment

Your system security plan, checking your controls and tracking fixes on a POA&M.

REQ.	REQUIREMENT	POINTS	STATUS
3.12.1	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. Can't go on a POA&M for Conditional Level 2	3	☐ Met ☐ Not met ☐ Unsure
3.12.3	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.12.4	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. Can't go on a POA&M for Conditional Level 2 No points, but required: without a system security plan there is no valid score.	0	☐ Met ☐ Not met ☐ Unsure

13 System and Communications Protection

Firewalls, network boundaries, encryption and secure communications.

REQ.	REQUIREMENT	POINTS	STATUS
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.13.3	Separate user functionality from system management functionality.	1	☐ Met ☐ Not met ☐ Unsure
3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.	1	☐ Met ☐ Not met ☐ Unsure
3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.13.7	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).	1	☐ Met ☐ Not met ☐ Unsure
3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. Can't go on a POA&M for Conditional Level 2	3	☐ Met ☐ Not met ☐ Unsure
3.13.9	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	1	☐ Met ☐ Not met ☐ Unsure
3.13.10	Establish and manage cryptographic keys for cryptography employed in organizational systems.	1	☐ Met ☐ Not met ☐ Unsure
3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. Partial credit: −3 instead of −5	5	☐ Met ☐ Not met ☐ Unsure
3.13.12	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	1	☐ Met ☐ Not met ☐ Unsure
3.13.13	Control and monitor the use of mobile code.	1	☐ Met ☐ Not met ☐ Unsure
3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	1	☐ Met ☐ Not met ☐ Unsure
3.13.15	Protect the authenticity of communications sessions. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.13.16	Protect the confidentiality of CUI at rest.	1	☐ Met ☐ Not met ☐ Unsure

14 System and Information Integrity

Patching, malware protection, security alerts and monitoring.

REQ.	REQUIREMENT	POINTS	STATUS
3.14.1	Identify, report, and correct system flaws in a timely manner. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.14.2	Provide protection from malicious code at designated locations within organizational systems. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.14.3	Monitor system security alerts and advisories and take action in response. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.14.4	Update malicious code protection mechanisms when new releases are available. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.14.5	Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed. Can't go on a POA&M for Conditional Level 2	3	☐ Met ☐ Not met ☐ Unsure
3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. Can't go on a POA&M for Conditional Level 2	5	☐ Met ☐ Not met ☐ Unsure
3.14.7	Identify unauthorized use of organizational systems. Can't go on a POA&M for Conditional Level 2	3	☐ Met ☐ Not met ☐ Unsure

SCORECARD

Estimate your SPRS score.

Add up the points for every requirement marked not met in each family, then subtract the total from 110. The lowest possible score is −203.

FAMILY	REQUIREMENTS	POINTS LOST
01 · Access Control	22	–
02 · Awareness and Training	3	–
03 · Audit and Accountability	9	–
04 · Configuration Management	9	–
05 · Identification and Authentication	11	–
06 · Incident Response	3	–
07 · Maintenance	6	–
08 · Media Protection	9	–
09 · Personnel Security	2	–
10 · Physical Protection	6	–
11 · Risk Assessment	3	–
12 · Security Assessment	4	–
13 · System and Communications Protection	16	–
14 · System and Information Integrity	7	–
Estimated SPRS score: 110 – points lost	**110**	

110

Every requirement met — the score a final Level 2 assessment requires.

88+

The bar for Conditional Level 2 status, if every open item can go on a POA&M.

Under 88

Below the 88 needed for Conditional Level 2 status.

No SSP

No system security plan (3.12.4): without one there’s no valid score to submit.

WANT AN ENGINEER TO CHECK IT FOR REAL?

A free CMMC gap assessment

Configured, not just installed
A self-check shows what's in place. We check whether it's set up well and actually monitored.

Plain-language report
We review your environment against the assessment objectives behind each requirement and hand you a scored SSP-ready gap list.

Discreet
We can work around your current provider and sign an NDA.

No obligation
Use the results with us, your current provider or anyone else.

Book at calitgroup.com/contact

866.24.CALIT

Point values from the NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1, which CMMC Level 2 scoring also uses. This is an estimate for planning — not an official assessment and not legal advice. Before you submit a score to SPRS or sign a CMMC affirmation, assess each requirement against its NIST SP 800-171A assessment objectives and keep the evidence.