CMMC Level 2 checklist: all 110 requirements, with their SPRS points

Use this to see where you stand before an assessment. Each requirement shows what it is worth on your SPRS score, whether it may be left open on a plan of action (POA&M), and whether it can be checked on your machines and systems or needs records that people keep.

How the score works.

- Start at **110**. Subtract each requirement that is not fully met: **5, 3, or 1 point**, as shown. Two requirements (3.5.3 and 3.13.11) give partial credit in specific cases. The lowest possible score is –203.
- **Conditional Level 2** needs a score of at least **88** (80% of 110), and every open requirement must be one that may go on a POA&M. Open items must be closed within **180 days**.
- Requirements marked **Must be met** may not be on a POA&M. Most are worth 5 points.
- No System Security Plan (3.12.4) means an assessment cannot be completed at all.

Machines = can be checked on your servers, computers, or connected systems such as Active Directory, Okta, Microsoft 365, or network devices. Other requirements are proven by policies and records people keep (list at the end).

Access Control (AC)

Done	ID	Requirement	Points	POA&M	Checked on
☐	3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	5	Must be met	Machines
☐	3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	5	Must be met	Machines
☐	3.1.3	Control the flow of CUI in accordance with approved authorizations.	1	Allowed	Machines
☐	3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	1	Allowed	Machines
☐	3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	3	Must be met	Machines
☐	3.1.6	Use non-privileged accounts or roles when accessing nonsecurity functions	1	Allowed	Machines
☐	3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	1	Allowed	Machines
☐	3.1.8	Limit unsuccessful logon attempts.	1	Allowed	Machines
☐	3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	1	Allowed	Machines
☐	3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity	1	Allowed	Machines
☐	3.1.11	Terminate (automatically) a user session after a defined condition.	1	Allowed	Machines
☐	3.1.12	Monitor and control remote access sessions.	5	Must be met	Machines
☐	3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	5	Must be met	Machines
☐	3.1.14	Route remote access via managed access control points.	1	Allowed	Machines
☐	3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	1	Allowed	Machines
☐	3.1.16	Authorize wireless access prior to allowing such connections	5	Must be met	Records
☐	3.1.17	Protect wireless access using authentication and encryption	5	Must be met	Records

☐	3.1.18	Control connection of mobile devices.	5	**Must be met**	Records
☐	3.1.19	Encrypt CUI on mobile devices and mobile computing platforms.	3	**Must be met**	Records
☐	3.1.20	Verify and control/limit connections to and use of external systems.	1	**Must be met**	Records
☐	3.1.21	Limit use of portable storage devices on external systems.	1	Allowed	Records
☐	3.1.22	Control CUI posted or processed on publicly accessible systems.	1	**Must be met**	Records

Awareness and Training (AT)

Done	ID	Requirement	Points	POA&M	Checked on
☐	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.	5	**Must be met**	**Machines**
☐	3.2.2	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	5	**Must be met**	**Machines**
☐	3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	1	Allowed	**Machines**

Audit and Accountability (AU)

Done	ID	Requirement	Points	POA&M	Checked on
☐	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	5	**Must be met**	**Machines**
☐	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.	3	**Must be met**	**Machines**
☐	3.3.3	Review and update logged events.	1	Allowed	Records
☐	3.3.4	Alert in the event of an audit logging process failure.	1	Allowed	**Machines**
☐	3.3.5	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	5	**Must be met**	**Machines**
☐	3.3.6	Provide audit record reduction and report generation to support on-demand analysis and reporting.	1	Allowed	**Machines**
☐	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	Allowed	**Machines**
☐	3.3.8	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	1	Allowed	**Machines**
☐	3.3.9	Limit management of audit logging functionality to a subset of privileged users.	1	Allowed	**Machines**

Configuration Management (CM)

Done	ID	Requirement	Points	POA&M	Checked on
☐	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.	5	**Must be met**	**Machines**
☐	3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational systems.	5	**Must be met**	**Machines**
☐	3.4.3	Track, review, approve or disapprove, and log changes to organizational systems.	1	Allowed	**Machines**

☐	3.4.4	Analyze the security impact of changes prior to implementation.	1	Allowed	Machines
☐	3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	5	Must be met	Machines
☐	3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	5	Must be met	Machines
☐	3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	5	Must be met	Machines
☐	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.	5	Must be met	Machines
☐	3.4.9	Control and monitor user-installed software.	1	Allowed	Machines

Identification and Authentication (IA)

Done	ID	Requirement	Points	POA&M	Checked on
☐	3.5.1	Identify system users, processes acting on behalf of users, and devices.	5	Must be met	Machines
☐	3.5.2	Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	5	Must be met	Machines
☐	3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. .	5	Must be met	Machines
☐	3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	1	Allowed	Machines
☐	3.5.5	Prevent reuse of identifiers for a defined period.	1	Allowed	Records
☐	3.5.6	Disable identifiers after a defined period of inactivity.	1	Allowed	Machines
☐	3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	1	Allowed	Machines
☐	3.5.8	Prohibit password reuse for a specified number of generations.	1	Allowed	Machines
☐	3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.	1	Allowed	Machines
☐	3.5.10	Store and transmit only cryptographically-protected passwords.	5	Must be met	Machines
☐	3.5.11	Obscure feedback of authentication information	1	Allowed	Machines

Incident Response (IR)

Done	ID	Requirement	Points	POA&M	Checked on
☐	3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	5	Must be met	Machines
☐	3.6.2	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	5	Must be met	Machines
☐	3.6.3	Test the organizational incident response capability.	1	Allowed	Records

Maintenance (MA)

Done	ID	Requirement	Points	POA&M	Checked on
☐	3.7.1	Perform maintenance on organizational systems..	3	Must be met	Machines
☐	3.7.2	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	5	Must be met	Machines
☐	3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	1	Allowed	Records

☐	3.7.4	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	3	**Must be met**	**Machines**
☐	3.7.5	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	5	**Must be met**	**Machines**
☐	3.7.6	Supervise the maintenance activities of maintenance personnel without required access authorization.	1	Allowed	Records

Media Protection (MP)

Done	ID	Requirement	Points	POA&M	Checked on
☐	3.8.1	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	3	**Must be met**	Records
☐	3.8.2	Limit access to CUI on system media to authorized users	3	**Must be met**	Records
☐	3.8.3	Sanitize or destroy system media containing CUI before disposal or release for reuse.	5	**Must be met**	Records
☐	3.8.4	Mark media with necessary CUI markings and distribution limitations.	1	Allowed	Records
☐	3.8.5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	1	Allowed	Records
☐	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	Allowed	**Machines**
☐	3.8.7	Control the use of removable media on system components.	5	**Must be met**	**Machines**
☐	3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.	3	**Must be met**	**Machines**
☐	3.8.9	Protect the confidentiality of backup CUI at storage locations.	1	Allowed	**Machines**

Personnel Security (PS)

Done	ID	Requirement	Points	POA&M	Checked on
☐	3.9.1	Screen individuals prior to authorizing access to organizational systems containing CUI.	3	**Must be met**	Records
☐	3.9.2	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers	5	**Must be met**	**Machines**

Physical Protection (PE)

Done	ID	Requirement	Points	POA&M	Checked on
☐	3.10.1	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	5	**Must be met**	Records
☐	3.10.2	Protect and monitor the physical facility and support infrastructure for organizational systems.	5	**Must be met**	Records
☐	3.10.3	Escort visitors and monitor visitor activity.	1	**Must be met**	Records
☐	3.10.4	Maintain audit logs of physical access.	1	**Must be met**	Records
☐	3.10.5	Control and manage physical access devices.	1	**Must be met**	Records
☐	3.10.6	Enforce safeguarding measures for CUI at alternate work sites.	1	Allowed	Records

Risk Assessment (RA)

Done	ID	Requirement	Points	POA&M	Checked on

☐	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	3	**Must be met**	Records
☐	3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	5	**Must be met**	**Machines**
☐	3.11.3	Remediate vulnerabilities in accordance with risk assessments.	1	Allowed	**Machines**

Security Assessment (CA)

Done	ID	Requirement	Points	POA&M	Checked on
☐	3.12.1	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	5	**Must be met**	**Machines**
☐	3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	3	**Must be met**	**Machines**
☐	3.12.3	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	5	**Must be met**	**Machines**
☐	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.	Required	**Must be met**	**Machines**

System and Communications Protection (SC)

Done	ID	Requirement	Points	POA&M	Checked on
☐	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.	5	**Must be met**	**Machines**
☐	3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	5	**Must be met**	Records
☐	3.13.3	Separate user functionality from system management functionality.	1	Allowed	**Machines**
☐	3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.	1	Allowed	**Machines**
☐	3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	5	**Must be met**	Records
☐	3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	5	**Must be met**	**Machines**
☐	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	Allowed	**Machines**
☐	3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	3	**Must be met**	**Machines**
☐	3.13.9	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	1	Allowed	**Machines**
☐	3.13.10	Establish and manage cryptographic keys for cryptography employed in organizational systems.	1	Allowed	**Machines**
☐	3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	5	Partial only	**Machines**

☐	3.13.12	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device..	1	Allowed	Records
☐	3.13.13	Control and monitor the use of mobile code.	1	Allowed	**Machines**
☐	3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	1	Allowed	Records
☐	3.13.15	Protect the authenticity of communications sessions.	5	**Must be met**	**Machines**
☐	3.13.16	Protect the confidentiality of CUI at rest.	1	Allowed	**Machines**

System and Information Integrity (SI)

Done	ID	Requirement	Points	POA&M	Checked on
☐	3.14.1	Identify, report, and correct system flaws in a timely manner.	5	**Must be met**	**Machines**
☐	3.14.2	Provide protection from malicious code at designated locations within organizational systems.	5	**Must be met**	**Machines**
☐	3.14.3	Monitor system security alerts and advisories and take action in response.	5	**Must be met**	**Machines**
☐	3.14.4	Update malicious code protection mechanisms when new releases are available.	5	**Must be met**	**Machines**
☐	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.	3	**Must be met**	**Machines**
☐	3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	5	**Must be met**	**Machines**
☐	3.14.7	Identify unauthorized use of organizational systems.	3	**Must be met**	**Machines**

The 17 records people keep

These are what an assessor asks for that no machine can prove. Most need a date, a name, and a signature.

Done	Record	What it shows	Who	How often
☐	**Security awareness training records**	Each person's completion of security awareness training, including insider threat awareness, with the date: before they get access, and every year. (3.2.1, 3.2.2, 3.2.3)	HR	every year
☐	**Training for administrators**	Records of role-based security training for administrators and others with security duties. (3.2.2)	IT	every year
☐	**Background checks before access**	Proof that everyone who handles CUI was screened before getting access. A list of names and dates is enough; HR keeps the reports. (3.9.1)	HR	once, then as it changes
☐	**Termination and transfer checklists**	For each person who left or changed roles: accounts disabled, and equipment and badges returned, with dates. (3.9.2)	HR	every quarter
☐	**Access review**	A signed review of who has access to systems with CUI, and what access was removed. (3.1.1, 3.1.2, 3.1.5, 3.1.7)	Security lead	every quarter
☐	**Visitor log**	Who visited areas where CUI is handled, when, and who escorted them. (3.10.3, 3.10.4)	Facilities	every quarter
☐	**Physical access list and badge inventory**	Who has keys, badges, or codes to areas with CUI, who approved it, and when codes or locks were last changed. (3.10.1, 3.10.2, 3.10.5)	Facilities	every year
☐	**Remote work rules, signed**	Each remote worker's signed acknowledgment of the rules for working with CUI at home or other sites. (3.10.6)	HR	every year
☐	**Maintenance log**	Maintenance on systems with CUI: by whom and when, remote sessions, and escort of outside technicians. (3.7.1, 3.7.2, 3.7.5, 3.7.6)	IT	every quarter

☐	**Media wiped or destroyed**	Drives, paper, and equipment with CUI that were wiped or destroyed: what, how, when, and by whom. (3.7.3, 3.8.3)	IT	every year
☐	**Inventory of media with CUI**	Removable drives, backups, and paper holding CUI: where each is kept and how it is marked. (3.8.1, 3.8.2, 3.8.4)	Security lead	every year
☐	**Incident response plan**	The plan, with roles and contacts, including reporting to the DoD within 72 hours (DFARS 252.204-7012). (3.6.1, 3.6.2)	Security lead	every year
☐	**Incident response test**	A record of a tabletop exercise or test of the plan: date, scenario, who took part, and what was improved. (3.6.3)	Security lead	every year
☐	**Risk assessment**	The periodic risk assessment of operations, assets, and people, and who approved it. (3.11.1)	Leadership	every year
☐	**Network diagram**	A diagram of the CUI boundary: its systems and every connection in and out. (3.13.1, 3.13.5)	IT	every year
☐	**Log review records**	Who reviewed the audit logs, when, what they looked at, and what was followed up. (3.3.3, 3.3.5)	IT	every month
☐	**Public content review**	Who reviews content before it goes on public websites, and a record of those reviews. (3.1.22)	Leadership	every year

Doing the technical side faster. Gardience checks the requirements marked **Machines** on your Windows and Linux servers and computers, fixes most failing settings with one approved click, keeps your SPRS score live, and writes the System Security Plan, the POA&M, and a signed evidence pack. People still own policy, training, and physical security, and an authorized assessor (C3PAO) performs the assessment. Free for 90 days on up to 25 machines: **gardience.com/trial**. A 15-minute walkthrough: **george@gardience.com**.

Requirement text: NIST SP 800-171 Rev. 2. Points: DoD Assessment Methodology as adopted in 32 CFR 170.24. POA&M rules: 32 CFR 170.21. This checklist is guidance, not legal advice or an assessment. © 2026 Bouziden Management LLC, d/b/a Gardience.