PLAYBOOK · NIST SP 800-171 · DCMA DIBCAC

Getting ready for a DIBCAC assessment

A plain-English guide for small defense contractors: what the assessors ask for, how they score you, and how to organize your proof so you can find any document in minutes.

Prepared by Sadler Enterprises LLC · Updated November 4, 2026 · Checked against DIBCAC's pre-assessment package, its C3PAO package, its public self-assessment database, and the DoD Assessment Methodology v1.2.1

110 security requirements in NIST SP 800-171	**320** assessment objectives, the checkpoints assessors grade
−203 lowest possible score, from a starting 110	**103** requirements that need more than paperwork

> **What this is not.** Legal advice, or a promise that you will pass. Your contract, your contracting officer, and the assessors have the final word. Source labels: Primary marks DoD or DCMA documents and federal regulation; Secondary marks commentary.

1. The big picture

If your company handles Controlled Unclassified Information (CUI) on a Department of Defense contract, you are expected to follow the 110 security requirements in NIST SP 800-171. Each requirement is split into smaller checkpoints called assessment objectives. DIBCAC's database holds 320 of them, and assessors grade you checkpoint by checkpoint.

DIBCAC is the Defense Industrial Base Cybersecurity Assessment Center, the government's own assessment team inside the Defense Contract Management Agency (DCMA). It does not sell services. It checks whether contractors do what their System Security Plan says they do.

Where things stand in November 2026

- DoD suspended CMMC Phase 2 in July 2026. The memo is effective immediately, and says DoD will enforce baseline compliance "through CMMC Level 1 and CMMC Level 2 self-assessment and select Government-led assessments." Primary
- What paused is the requirement for program offices to designate CMMC Level 2 (C3PAO) assessments, along with CMMC Level 3 (DIBCAC) designations, during a 60-day review. The memo says further guidance will follow that review. Primary
- What did not pause: DFARS 252.204-7012 "remain[s] in effect," so the 110 requirements still apply. Basic self-assessments and SPRS scores still apply, and so do CMMC Level 1 and Level 2 (Self) assessments. Where your contract has DFARS 252.204-7021, you must keep a current CMMC status for the life of the contract and complete an affirmation of continuous compliance in SPRS every year. A Level 2 (Self) status is good for 3 years. Primary That the suspension leaves self-assessments and SPRS scores in place is from a law-firm summary. Secondary
- DFARS 252.204-7020 requires you to give the Government access to your facilities, systems and personnel for a Medium or High assessment. The memo does not mention it. Primary This is separate from CMMC Level 3. The copy of the clause we reviewed (NOV 2023) is filed under a "reserved" parent topic, which fits reports that it was renumbered, so check which clause number your contract cites.
- **Our planning assumption:** DIBCAC assessments under your contract are not suspended, and C3PAO assessments are likely to return. DoD has not said when. Prepare as if either could be scheduled.
- As of November 4, 2026, we found no announcement ending the suspension. Check the DoD CIO CMMC page for anything newer.
- Practical result: your self-assessment score and your SSP carry more weight, not less. Treat them as if an assessor will read them.

2. Three kinds of assessment

Level	Who does it	What happens	What it feels like
Basic	You	You score yourself against the 110 requirements and post the score in SPRS.	Homework you grade yourself.
Medium	DIBCAC	Assessors review your self-assessment and System Security Plan (SSP) on paper. If the SSP does not clearly show how a requirement is met, it is scored "Not Implemented."	A teacher checking your homework.

Level	Who does it	What happens	What it feels like
High	DIBCAC	Everything in Medium, plus artifact requests, interviews with your people, and live demonstrations. A virtual portion, and sometimes an on-site portion. Scheduled Monday to Thursday, with Friday held in reserve.	An open-book exam with a live demonstration.

DFARS 252.204-7020 defines both as Government assessments. A Medium assessment is a review of your Basic assessment, a thorough document review, and discussions with you. A High assessment adds verification, examination and demonstration of your SSP using NIST SP 800-171A. Primary

The methodology rates the resulting score by confidence: Low for a Basic (self-generated) score, Medium for a Medium assessment, and High for a High assessment. It describes Medium assessments as conducted by trained DoD personnel, often program office staff; DIBCAC's package covers the DIBCAC-run version. Primary

Source: DIBCAC Pre-Assessment Package, Enclosure 1. Primary NIST SP 800-171A is named there as the primary and authoritative guide for assessing the requirements.

---

3. How scoring works

You start at 110. For each requirement you have not fully met, you subtract its point value. A score below zero is possible and is not unusual for a first honest self-assessment.

Point value	Requirements	Examples
5 points	44	Limiting access (3.1.1), multifactor authentication (3.5.3), flaw remediation (3.14.1), baseline configurations (3.4.1)
3 points	14	Least privilege (3.1.5), risk assessment (3.11.1), unique user traceability (3.3.2)
1 point	51	Session lock (3.1.10), reviewing logged events (3.3.3), testing incident response (3.6.3)
0 points	1	System Security Plan (3.12.4)

Floor: 44×5 + 14×3 + 51×1 = 313 points, so the lowest score is 110 − 313 = **−203**.

The SSP (3.12.4) carries no points, but without it there is nothing to score. The methodology says the absence of an SSP results in a finding that "an assessment could not be completed due to incomplete information and noncompliance with DFARS clause 252.204-7012." Primary

Partial credit and "does not apply" rules

Source: DoD Assessment Methodology v1.2.1 (June 24, 2020) and DIBCAC's self-assessment database. Scoring is the same for Basic, Medium and High assessments. Primary

Requirement	Rule written into DIBCAC's database
3.5.3 Multifactor authentication	Subtract 5 if MFA is not implemented for any users. Subtract 3 if MFA is implemented only for remote and privileged users and not yet for general users. Primary

Requirement	Rule written into DIBCAC's database
3.13.11 FIPS-validated cryptography	Subtract 5 if no cryptography is employed. Subtract 3 if it is employed but not FIPS-validated. The cryptographic module must be validated under FIPS 140; using an approved algorithm such as AES is not enough. Isolated non-validated use with a plan of action is treated as a temporary deficiency and scored as implemented. Primary
3.1.12, 3.1.13 Remote access	No deduction if remote access is not permitted.
3.1.16, 3.1.17 Wireless	No deduction if wireless access is not permitted.
3.1.18 Mobile devices	No deduction if connection of mobile devices is not permitted. The methodology adds that a company that disallows remote, wireless or mobile access should also have a policy and procedure ensuring those capabilities are not enabled inadvertently. Without one, a point can be assessed.

Four rules that surprise people

- **A plan of action earns no credit.** A requirement that is not fully implemented is scored "not implemented," whether or not a plan exists. The methodology's own example is an MFA rollout that is 75% complete: 3.5.3 is still "not implemented."
- **No plan of action, no 3.12.2.** Missing plans of action for unimplemented requirements make 3.12.2 itself "not implemented."
- **Temporary deficiencies can still score as implemented.** If a plan of action has milestones and shows progress, for example a patch that broke a FIPS validation or a rollout held up by unexpected hardware issues, the requirement can be scored as implemented. There is no standard duration; it is "what is reasonable."
- **Isolated enduring exceptions can too.** Unique equipment, such as specialized manufacturing gear or a laboratory, that cannot meet a requirement is assessed as implemented when the exception and its mitigations are described in the SSP.

Source: DoD Assessment Methodology v1.2.1, sections 5(g) and 5(h). Primary

> **Takeaway.** A 5-point requirement you skip costs as much as five 1-point requirements. Fix the 5-pointers first. The appendix lets you mark requirements as not met and see the resulting score.

4. The four kinds of proof

For each of the 320 checkpoints, DIBCAC's database records the kind of proof assessors expect to see.



Document **126** Artifact **82** Screen Share **93** Physical Review **18** Artifact + Screen Share **1**

Proof type	What it means for you	Everyday examples
Document	Something written down and approved.	Policies, procedures, the SSP, a network diagram, a list of authorized users
Artifact	A record showing the thing actually happened.	Training sign-in sheets, access-review records, scan reports, patch tickets, log-review notes, an incident-response exercise write-up
Screen Share	Show it live on screen.	Logging in with MFA, a locked-down account, a firewall rule, an encryption setting
Physical Review	The assessor sees it in person.	Locked doors, visitor log, escorted visitors, secured storage, media markings
Artifact + Screen Share	Both. This is 3.13.11, FIPS-validated cryptography.	The validation certificate and the setting turned on

Counts come from the "Standard" column of DIBCAC's Public 800-171 Self-Assessment Database v1.1. The database does not define the terms; the examples are ours.

> **A binder of policies is the starting line**
>
> Only 7 of the 110 requirements can be satisfied by paperwork alone: 3.1.21, 3.5.1, 3.5.9, 3.6.1, 3.7.6, 3.8.3, and the SSP itself (3.12.4). For the other 103, at least one checkpoint needs a record, a live demonstration, or an in-person look.

What makes your proof acceptable

1. **Explain how you do it; do not copy the requirement.** Pasting the NIST wording into the SSP is called out as not acceptable. Say how, with what, and who does it. Primary
2. **Connect each tool or policy to the requirement.** "We use Microsoft 365" is not an answer. "MFA is enforced for all users through Conditional Access policy X" is. Primary
3. **Have everything the SSP mentions ready.** Supporting documentation referenced in the SSP should be available to the assessment team. Primary
4. **Send the current, final SSP** and keep a revision history for the SSP and key artifacts. Primary
5. **Keep artifacts unaltered.** Be able to show a file is the same as when the assessor reviewed it (see section 8). Primary

---

5. What DIBCAC will ask you for

For both Medium and High assessments

- [ ] **Your Basic self-assessment**, with the total score for each SSP (for example, 105 of 110) and the date you expect to reach 110.

- [ ] **The score posted in SPRS.** Access is through PIEE; your company's Contractor Administrator (CAM) adds the "SPRS Cyber Vendor" role for whoever enters it.
- [ ] **Your System Security Plan(s)** covering a general system description, system boundaries, environments of operation, major applications, general support systems, minor applications, how each of the 110 requirements is implemented, connections to other systems (including mission partners), and revision history.
- [ ] **Plans of Action** for every requirement your Basic assessment shows as not implemented.
- [ ] **The CAGE / Contract Verification sheet (Enclosure 2)**, signed by a company official.
  Digital signature. Send both a PDF and the Excel file, and do not password-protect either.

What Enclosure 2 contains

Tables 1 and 3–4

- SSP name and version, Basic score, assessment date, and the date you expect 110. All must match SPRS.
- **Three high-priority contracts** (preferably active) containing DFARS 252.204-7012, and 252.204-7020 if applicable. Say whether each contains CUI.
- **Every CAGE code** your company has, whether or not DCMA administers it, and whether each is covered by the enterprise SSP.

Table 2: ten yes / no / N/A attestations

Each one initialed by the company official.

- 7012(b)(2)(ii)(D): external cloud service requirements
- 7012(c): cyber incident reporting
- 7012(d): malicious software
- 7012(e): media preservation and protection
- 7012(f): access to additional information or equipment
- 7012(g): cyber incident damage assessment
- 7012(h): safeguarding contractor attributional or proprietary information
- 7012(m)(1): flow-down clause in subcontracts
- 7012(m)(1): CUI determination in subcontracts by the prime
- 7012(m)(2): notification and incident report requirement

The signature states that the listed CAGE codes are covered by the named SSP and are in scope. The sheet warns that re-assessment may be required if changes are requested after the assessment.

Additional items for a High assessment

- [ ] **A detailed network diagram** of where CUI lives and travels, showing as applicable: security boundaries, cybersecurity stack, security event management, connections to other networks, cloud connections and data flow, wireless (802.11), point-to-point links, MPLS, high-level IP scheme, critical network services, vulnerability scanning approach, authentication, enterprise logging, remote access, how a remote user browses the web, DNS, VoIP, and video.
- [ ] **Artifacts** for any requirement met by a policy, process, or manual log.
- [ ] **Governance proof.** How your enterprise SSP flows down to individual contracts (assessors sample contracts), policies for isolated networks or labs, and internal audit records, if you have them.
- [ ] **Evidence for the rest of DFARS 252.204-7012:** cloud computing, cyber incident reporting, and damage assessment.
- [ ] **People available for interviews** by role (see section 7), including the team that maintains your 7012 policies.
- [ ] **Screen-share capability.** If you prefer a collaboration tool, name it before the pre-assessment coordination call.

If you are a subcontractor, or you hire them

- DFARS 252.204-7020 must be flowed down in all subcontracts, including for commercial products and services, except commercially available off-the-shelf items.
- A prime may not award a subcontract subject to 252.204-7012 unless the subcontractor has completed at least a Basic assessment within the last 3 years. A posted score older than 3 years does not count unless the solicitation sets a shorter period.
- SPRS holds the summary score, such as 105 of 110, not the score for each requirement. DoD keeps any extra High-assessment documentation as CUI for internal use.

Source: DFARS 252.204-7020 (NOV 2023), paragraphs (d), (f) and (g). Primary

Small-business reality check. DIBCAC's list was written for companies of every size. In a ten-person shop, one person may be the network administrator, the account manager, and the incident responder. That is fine, as long as that person can explain and demonstrate each area.

6. Timeline

When	What happens	Your job
5 weeks before	Pre-assessment coordination call	Have your self-assessment score, SSP, and Enclosure 2 ready
14 days before	DIBCAC sends a DoD SAFE drop request	Gather your files
7 days before	Materials received by DCMA	Upload, encrypted
By the last day	DCMA out-brief	Listen and take notes
14 business days after	Reclama period ends	Submit corrections or added evidence if you disagree with a finding. DFARS 252.204-7020(e)(2) gives you 14 business days to rebut.
Within 60 days after a High	Results provided to the company	Update SPRS and your plans of action

DIBCAC publishes this as a tentative schedule. Primary Candidate C3PAOs follow a different track: a scoping call about eight weeks out, SAFE uploads two weeks before the scoping call and before the start, and an agreed assessment plan at least three days ahead.

A High assessment week

Monday

In-brief, then assessors read your SSP and documents.

4:00–4:30 pm: artifact requests and hot wash.

Tuesday

Room 1: 3.1 Access Control, 3.3 Audit, 3.5 Identification & Authentication.

Room 2: 3.2, 3.9, 3.10, 3.11, 3.12.

Room 3: 3.4, 3.7, 3.8.

Wednesday

Room 1: 3.6 Incident Response, 3.13 System & Communications Protection, 3.14 System & Information Integrity.

Rooms 2 and 3 continue their Tuesday families.

Thursday

Follow-ups in all rooms, final artifact request if required, then the out-brief.

Friday is held in reserve.

> **Expect homework every day.** Assessors issue artifact requests at midday and at the end of each day. Being able to find any document in minutes is the most practical thing you can prepare.

7. Who needs to be available

DIBCAC asks for subject matter experts who can demonstrate implementation and answer questions for each security family. Write a real name next to each role, even if it is the same name several times.

DIBCAC role	Related families (our mapping)	Who in your company?
Network administrator / engineer	3.1, 3.13	Name: _____
Account management / Active Directory administrator	3.1, 3.5	Name: _____
Audit and logging responsibilities	3.3	Name: _____
Cybersecurity / IT policy oversight	All	Name: _____
Information security responsibilities / senior information security officer	3.12, 3.14	Name: _____
Configuration management	3.4	Name: _____
Cyber net defender / incident response	3.6	Name: _____
Risk assessment team	3.11	Name: _____
Personnel / human resources, training	3.2, 3.9	Name: _____
Physical security specialist	3.10	Name: _____
Access enforcement personnel	3.1	Name: _____
System developers (if any)	3.13	Name: _____
Enterprise services lead	3.7, 3.8, 3.13	Name: _____

Roles are the list in DIBCAC Enclosure 1. If an outside IT or security provider runs part of your environment, add their contact as well; that line is our suggestion, not DIBCAC's.

8. Packaging and sending your proof

DIBCAC transfers files through DoD SAFE, a government file-exchange service approved for CUI and PII. It accepts up to 8 GB, and it deletes files after 7 days.

1. **Encrypt every file.** The "Encrypt every file" box is required.
2. **Use a passphrase of at least 10 characters.** Give it to the Assessment Lead by a different channel, such as a phone call or a separate email.
3. **Name files the DIBCAC way.** High: requirement, objective, assessment number, company, date. Medium: assessment number, company, date.

High	`3.1.20_a_22-XXX_CompanyName_20220325`
Medium	`22-XXX_CompanyName_20220325`

4. **Organize by family.** One folder per family (3.1, 3.2, and so on), then zip the whole set into one file.
5. **Keep your own master copy.** SAFE deletes after 7 days, and the examples in DIBCAC's package are dated 2022, so confirm the current naming with your Assessment Lead.

> **If you pursue CMMC Level 2 certification**
>
> Under 32 CFR 170.17(c)(4), your company keeps the hashed assessment artifacts for **six years from the CMMC Status Date**. You hash the artifact files with a NIST-approved algorithm and give the C3PAO a list of file names, hash values, and the algorithm used. Keep originals untouched so any later change is evident. Primary

9. The ten requirements companies fail most

DIBCAC's own data from 117 High assessments (2019 to 2022). These ten were among 883 total "Other Than Satisfied" findings.

#	Requirement	Points	Share of companies with the finding	Proof expected	In plain English
1	**3.13.11** FIPS-validated encryption	5 (or 3)	**50%** 58 findings	Artifact + Screen Share	Encrypting is not enough. The module must be government-validated. Ask vendors for the certificate number.
2	**3.5.3** Multifactor authentication	5 (or 3)	**38%** 45 findings	Document, Screen Share	A second login factor for privileged accounts and network access, shown working.
3	**3.14.1** Find and fix flaws	5	**22%** 26 findings	Document, Screen Share	A defined patch process with timelines, and proof you follow it.
4	**3.11.1** Periodic risk assessment	3	**18%** 21 findings	Document, Artifact	A dated written assessment, repeated on schedule.
5	**3.11.2** Vulnerability scanning	5	**18%** 21 findings	Document, Screen Share	Scheduled scans, and the ability to show the tool and its results.
6	**3.3.3** Review logged events	1	**16%** 19 findings	Document, Artifact	Periodically decide whether you are logging the right things, and write down that you did.

#	Requirement	Points	Share of companies with the finding	Proof expected	In plain English
7	**3.3.4** Alert when logging fails	1	**15%** 18 findings	Document, Artifact	Someone is alerted if logging stops.
8	**3.3.5** Review and correlate logs	5	**15%** 18 findings	Document, Artifact	Someone reads the logs and acts on what they find.
9	**3.6.3** Test incident response	1	**15%** 18 findings	Artifact	Run a drill or tabletop exercise and keep the write-up.
10	**3.4.1** Baseline configurations	5	**15%** 17 findings	Document, Artifact	A documented standard build for each device type, and an up-to-date inventory.

> **Pattern to notice.** Most of these failures are not missing policies. They are missing proof that something happens regularly: reviews, scans, drills, alerts. Build a calendar and keep the records.

Source: DCMA DIBCAC, *Top "Other Than Satisfied" Requirements from DIBCAC High Assessments* (December 2022). The data covers 117 High assessments from 2019 to 2022 and 883 total findings; these ten account for 261 of them. Points and proof types match the self-assessment database. Primary

---

10. Two templates worth borrowing

DIBCAC's separate package for companies applying to become C3PAOs is not meant for ordinary contractors, but two of its templates are good models for any business.

Asset inventory, in five categories

Category	Plain English	Example
CUI asset	Stores, processes, or sends CUI	Laptops used for contract work; cloud file storage
Security protection asset	Provides security functions for your scope, whether or not it touches CUI	Identity system, MFA app, firewall, a managed IT provider's staff
Contractor risk managed asset	Could touch CUI, but policy and practice keep it from doing so. It does not have to be separated from CUI assets.	A thumb drive that policy forbids using for CUI
Specialized asset	Government property, IoT, operational technology, restricted systems, test equipment	A networked CNC machine
Out of scope	Cannot touch CUI and is physically or logically separated from CUI assets	A separate phone system

Each entry lists the category, asset, quantity, type, and a one-line description. The template is optional; a corporate inventory format is acceptable if it covers the same categories.

Inherited and not-applicable list

- **Inherited:** someone else does it for you, such as a cloud provider inside its own service. You still need their customer responsibility matrix as proof.
- **Partially inherited:** they handle some objectives and you handle the rest.
- **Not applicable:** it truly does not apply. Write a one-line reason. Example: "Wireless access is not permitted by policy."

11. A simple preparation plan

- [ ] Find out what your contracts require. Look for DFARS 252.204-7012 and any CMMC clause.
- [ ] List every system, person, and provider that touches CUI, using the five asset categories.
- [ ] Draw a simple diagram of where CUI lives and travels.
- [ ] Write or update the SSP: how you meet each requirement, in your own words.
- [ ] Score yourself honestly and write a plan of action for every gap.
- [ ] Fix the 5-point requirements and the top ten first.
- [ ] For every checkpoint, file the proof type DIBCAC expects (see the appendix).
- [ ] Name and organize files the DIBCAC way, and keep a protected master copy.
- [ ] Post your score in SPRS and set a recurring calendar for reviews, scans, and drills.
- [ ] Rehearse: can each person in section 7 show their area live in under five minutes?

Appendix: all 110 requirements

Points, objective counts, and proof types come straight from DIBCAC's self-assessment database.

Proof key: D = Document, A = Artifact, S = Screen Share, P = Physical Review, A+S = both. "D×3, S×3" means three checkpoints need a document and three need a live demonstration.

3.1 Access Control

3.1.1 AC.L1-3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	**5 pt** 6 objectives · D×3, S×3
3.1.2 AC.L1-3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	**5 pt** 2 objectives · D×1, S×1
3.1.3 AC.L2-3.1.3	Control the flow of CUI in accordance with approved authorizations.	**1 pt** 5 objectives · D×3, A×1, S×1
3.1.4 AC.L2-3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	**1 pt** 3 objectives · D×1, S×2
3.1.5 AC.L2-3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	**3 pt** 4 objectives · D×2, A×2
3.1.6 AC.L2-3.1.6	Use non-privileged accounts or roles when accessing nonsecurity functions.	**1 pt** 2 objectives · D×1, S×1
3.1.7 AC.L2-3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	**1 pt** 4 objectives · D×2, S×2
3.1.8 AC.L2-3.1.8	Limit unsuccessful logon attempts.	**1 pt** 2 objectives · D×1, A×1
3.1.9 AC.L2-3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	**1 pt** 2 objectives · D×1, A×1
3.1.10 AC.L2-3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	**1 pt** 3 objectives · D×2, A×1
3.1.11 AC.L2-3.1.11	Terminate (automatically) a user session after a defined condition.	**1 pt** 2 objectives · D×1, S×1
3.1.12 AC.L2-3.1.12	Monitor and control remote access sessions.	**5 pt** 4 objectives · D×2, S×2
3.1.13 AC.L2-3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	**5 pt** 2 objectives · D×1, S×1
3.1.14 AC.L2-3.1.14	Route remote access via managed access control points.	**1 pt** 2 objectives · S×2
3.1.15 AC.L2-3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	**1 pt** 4 objectives · D×2, A×2
3.1.16 AC.L2-3.1.16	Authorize wireless access prior to allowing such connections.	**5 pt** 2 objectives · D×1, S×1
3.1.17 AC.L2-3.1.17	Protect wireless access using authentication and encryption.	**5 pt** 2 objectives · S×2

3.1.18 AC.L2-3.1.18	Control connection of mobile devices. **5 pt** 3 objectives · D×1, A×1, S×1
3.1.19 AC.L2-3.1.19	Encrypt CUI on mobile devices and mobile computing platforms **3 pt** 2 objectives · D×1, S×1
3.1.20 AC.L1-3.1.20	Verify and control/limit connections to and use of external systems. **1 pt** 6 objectives · D×2, A×2, S×2
3.1.21 AC.L2-3.1.21	Limit use of portable storage devices on external systems. **1 pt** 3 objectives · D×3
3.1.22 AC.L1-3.1.22	Control CUI posted or processed on publicly accessible systems. **1 pt** 5 objectives · D×2, A×3
3.2 Awareness and Training	
3.2.1 AT.L2-3.2.1	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 pt** 4 objectives · D×2, A×2
3.2.2 AT.L2-3.2.2	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. **5 pt** 3 objectives · D×1, A×2
3.2.3 AT.L2-3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat. **1 pt** 2 objectives · D×1, A×1
3.3 Audit and Accountability	
3.3.1 AU.L2-3.3.1	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 pt** 6 objectives · D×3, S×3
3.3.2 AU.L2-3.3.2	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 pt** 2 objectives · D×1, S×1
3.3.3 AU.L2-3.3.3	Review and update logged events. **1 pt** 3 objectives · D×1, A×2
3.3.4 AU.L2-3.3.4	Alert in the event of an audit logging process failure. **1 pt** 3 objectives · D×2, A×1
3.3.5 AU.L2-3.3.5	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. **5 pt** 2 objectives · D×1, A×1
3.3.6 AU.L2-3.3.6	Provide audit record reduction and report generation to support on-demand analysis and reporting. **1 pt** 2 objectives · S×2
3.3.7 AU.L2-3.3.7	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records. **1 pt** 3 objectives · D×1, S×2

3.3.8 AU.L2-3.3.8	Protect audit information and audit logging tools from unauthorized access, modification, and deletion. **1 pt** 6 objectives · S×6
3.3.9 AU.L2-3.3.9	Limit management of audit logging functionality to a subset of privileged users. **1 pt** 2 objectives · D×1, S×1
3.4 Configuration Management	
3.4.1 CM.L2-3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. **5 pt** 6 objectives · D×2, A×4
3.4.2 CM.L2-3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational systems. **5 pt** 2 objectives · D×1, A×1
3.4.3 CM.L2-3.4.3	Track, review, approve or disapprove, and log changes to organizational systems. **1 pt** 4 objectives · A×4
3.4.4 CM.L2-3.4.4	Analyze the security impact of changes prior to implementation. **1 pt** 1 objective · A×1
3.4.5 CM.L2-3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems. **5 pt** 8 objectives · D×4, A×3, P×1
3.4.6 CM.L2-3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities. **5 pt** 2 objectives · D×1, S×1
3.4.7 CM.L2-3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. **5 pt** 15 objectives · D×10, S×5
3.4.8 CM.L2-3.4.8	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 pt** 3 objectives · D×2, S×1
3.4.9 CM.L2-3.4.9	Control and monitor user-installed software. **1 pt** 3 objectives · D×1, S×2
3.5 Identification and Authentication	
3.5.1 IA.L1-3.5.1	Identify system users, processes acting on behalf of users, and devices. **5 pt** 3 objectives · D×3
3.5.2 IA.L1-3.5.2	Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems. **5 pt** 3 objectives · S×3
3.5.3 IA.L2-3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. **5 pt** 4 objectives · D×1, S×3
3.5.4 IA.L2-3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. **1 pt** 1 objective · S×1

3.5.5 IA.L2-3.5.5	Prevent reuse of identifiers for a defined period. **1 pt** 2 objectives · D×1, A×1
3.5.6 IA.L2-3.5.6	Disable identifiers after a defined period of inactivity. **1 pt** 2 objectives · D×1, A×1
3.5.7 IA.L2-3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created. **1 pt** 4 objectives · D×2, S×2
3.5.8 IA.L2-3.5.8	Prohibit password reuse for a specified number of generations. **1 pt** 2 objectives · D×1, S×1
3.5.9 IA.L2-3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password. **1 pt** 1 objective · D×1
3.5.10 IA.L2-3.5.10	Store and transmit only cryptographically-protected passwords. **5 pt** 2 objectives · S×2
3.5.11 IA.L2-3.5.11	Obscure feedback of authentication information. **1 pt** 1 objective · S×1
3.6 Incident Response	
3.6.1 IR.L2-3.6.1	Establish an operational incident- handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. **5 pt** 7 objectives · D×7
3.6.2 IR.L2-3.6.2	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization. **5 pt** 6 objectives · D×2, A×3, S×1
3.6.3 IR.L2-3.6.3	Test the organizational incident response capability. **1 pt** 1 objective · A×1
3.7 Maintenance	
3.7.1 MA.L2-3.7.1	Perform maintenance on organizational systems. **3 pt** 1 objective · A×1
3.7.2 MA.L2-3.7.2	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. **5 pt** 4 objectives · A×3, P×1
3.7.3 MA.L2-3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI. **1 pt** 1 objective · A×1
3.7.4 MA.L2-3.7.4	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems. **3 pt** 1 objective · A×1
3.7.5 MA.L2-3.7.5	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. **5 pt** 2 objectives · S×2
3.7.6 MA.L2-3.7.6	Supervise the maintenance activities of maintenance personnel without required access authorization. **1 pt** 1 objective · D×1

3.8 Media Protection

3.8.1 MP.L2-3.8.1	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	**3 pt** 4 objectives · D×2, P×2
3.8.2 MP.L2-3.8.2	Limit access to CUI on system media to authorized users.	**3 pt** 1 objective · A×1
3.8.3 MP.L1-3.8.3	Sanitize or destroy system media containing CUI before disposal or release for reuse.	**5 pt** 2 objectives · D×2
3.8.4 MP.L2-3.8.4	Mark media with necessary CUI markings and distribution limitations.	**1 pt** 2 objectives · P×2
3.8.5 MP.L2-3.8.5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	**1 pt** 2 objectives · D×1, A×1
3.8.6 MP.L2-3.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	**1 pt** 1 objective · A×1
3.8.7 MP.L2-3.8.7	Control the use of removable media on system components.	**5 pt** 1 objective · A×1
3.8.8 MP.L2-3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.	**3 pt** 1 objective · A×1
3.8.9 MP.L2-3.8.9	Protect the confidentiality of backup CUI at storage locations.	**1 pt** 1 objective · A×1

3.9 Personnel Security

3.9.1 PS.L2-3.9.1	Screen individuals prior to authorizing access to organizational systems containing CUI.	**3 pt** 1 objective · A×1
3.9.2 PS.L2-3.9.2	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	**5 pt** 3 objectives · D×1, A×2

3.10 Physical Protection

3.10.1 PE.L1-3.10.1	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	**5 pt** 4 objectives · A×1, P×3
3.10.2 PE.L2-3.10.2	Protect and monitor the physical facility and support infrastructure for organizational systems.	**5 pt** 4 objectives · P×4
3.10.3 PE.L1-3.10.3	Escort visitors and monitor visitor activity.	**1 pt** 2 objectives · P×2
3.10.4 PE.L1-3.10.4	Maintain audit logs of physical access.	**1 pt** 1 objective · A×1

3.10.5 PE.L1-3.10.5	Control and manage physical access devices. **1 pt** 3 objectives · D×1, P×2
3.10.6 PE.L2-3.10.6	Enforce safeguarding measures for CUI at alternate work sites. **1 pt** 2 objectives · D×1, A×1
3.11 Risk Assessment	
3.11.1 RA.L2-3.11.1	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 pt** 2 objectives · D×1, A×1
3.11.2 RA.L2-3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. **5 pt** 5 objectives · D×1, S×4
3.11.3 RA.L2-3.11.3	Remediate vulnerabilities in accordance with risk assessments. **1 pt** 2 objectives · A×2
3.12 Security Assessment	
3.12.1 CA.L2-3.12.1	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. **5 pt** 2 objectives · D×1, A×1
3.12.2 CA.L2-3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. **3 pt** 3 objectives · A×3
3.12.3 CA.L2-3.12.3	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. **5 pt** 1 objective · A×1
3.12.4 CA.L2-3.12.4	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. **0 pt** 8 objectives · D×8
3.13 System and Communications Protection	
3.13.1 SC.L1-3.13.1	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 pt** 8 objectives · D×2, S×6
3.13.2 SC.L2-3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. **5 pt** 6 objectives · D×3, A×3
3.13.3 SC.L2-3.13.3	Separate user functionality from system management functionality. **1 pt** 3 objectives · D×2, S×1
3.13.4 SC.L2-3.13.4	Prevent unauthorized and unintended information transfer via shared system resources. **1 pt** 1 objective · S×1

3.13.5 SC.L1-3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. **5 pt** 2 objectives · D×1, A×1
3.13.6 SC.L2-3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). **5 pt** 2 objectives · S×2
3.13.7 SC.L2-3.13.7	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 pt** 1 objective · S×1
3.13.8 SC.L2-3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. **3 pt** 3 objectives · D×2, A×1
3.13.9 SC.L2-3.13.9	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. **1 pt** 3 objectives · D×1, S×2
3.13.10 SC.L2-3.13.10	Establish and manage cryptographic keys for cryptography employed in organizational systems. **1 pt** 2 objectives · A×2
3.13.11 SC.L2-3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. **5 pt** 1 objective · A+S×1
3.13.12 SC.L2-3.13.12	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device. **1 pt** 3 objectives · D×1, A×1, P×1
3.13.13 SC.L2-3.13.13	Control and monitor the use of mobile code. **1 pt** 2 objectives · S×2
3.13.14 SC.L2-3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies. **1 pt** 2 objectives · A×2
3.13.15 SC.L2-3.13.15	Protect the authenticity of communications sessions. **5 pt** 1 objective · S×1
3.13.16 SC.L2-3.13.16	Protect the confidentiality of CUI at rest. **1 pt** 1 objective · A×1
3.14 System and Information Integrity	
3.14.1 SI.L1-3.14.1	Identify, report, and correct system flaws in a timely manner. **5 pt** 6 objectives · D×3, S×3
3.14.2 SI.L1-3.14.2	Provide protection from malicious code at designated locations within organizational systems. **5 pt** 2 objectives · D×1, S×1

3.14.3 SI.L2-3.14.3	Monitor system security alerts and advisories and take action in response. **5 pt** 3 objectives · D×1, A×2
3.14.4 SI.L1-3.14.4	Update malicious code protection mechanisms when new releases are available. **5 pt** 1 objective · S×1
3.14.5 SI.L1-3.14.5	Perform periodic scans of organizational systems and real- time scans of files from external sources as files are downloaded, opened, or executed. **3 pt** 3 objectives · D×1, S×2
3.14.6 SI.L2-3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. **5 pt** 3 objectives · S×3
3.14.7 SI.L2-3.14.7	Identify unauthorized use of organizational systems **3 pt** 2 objectives · D×1, A×1

Sources

1. DoD CIO, *Implementing Suspension of CMMC Phase II* (July 2026). dodcio.defense.gov **Primary**
2. DFARS 252.204-7021, *Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements* (NOV 2025): current CMMC status, annual affirmation in SPRS, status validity periods. **Primary**
3. DFARS 252.204-7020, *NIST SP 800-171 DoD Assessment Requirements* (NOV 2023): access obligations, assessment definitions, SPRS posting, 14-business-day rebuttal, and subcontractor flow-down. **Primary**
4. DoD, *NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1* (June 24, 2020), including the scoring table and sections 4 to 6. Landing page: acq.osd.mil **Primary**
5. DCMA DIBCAC, *Pre-Assessment Documents for High and Medium NIST SP 800-171 Assessments*: Enclosure 1 (Action Items and Schedule), Enclosure 2 (CAGE/Contract Verification), Enclosure 3 (Assessment Logistics). dcma.mil **Primary**
6. DCMA DIBCAC, *Public High NIST SP 800-171 Self-Assessment Database, v1.1*: points, special scoring notes, and proof type for each of the 320 objectives. dcma.mil **Primary**
7. DCMA DIBCAC, *Pre-Assessment Package for Prospective C3PAO Assessments*: Planning Guide, Tab C (Inherited/N/A), Tab D (Asset Inventory). dcma.mil **Primary**
8. 32 CFR 170.17, CMMC Level 2 certification assessment, including paragraph (c)(4) on artifact hashing and six-year retention. ecfr.gov **Primary**
9. DCMA DIBCAC, *Top "Other Than Satisfied" Requirements from DIBCAC High Assessments* (December 2022). dcma.mil **Primary**
10. NIST SP 800-171 Rev. 2 and SP 800-171A. csrc.nist.gov **Primary**
11. Latham & Watkins, *What Defense Contractors Should Know About DOD's Suspension of CMMC Phase 2* (July 30, 2026). lw.com **Secondary**

The DCMA documents reviewed here were downloaded from DCMA on November 4, 2026. The Enclosure 1 and 3 files and the C3PAO planning guide carry 2022 dates, and Enclosure 2 was last updated in February 2025. If DIBCAC sends you newer templates for your assessment, use those.

Run the assessment on your own machine

Axiometrik is desktop software for CMMC 2.0 Level 2 (NIST SP 800-171 Rev 2) and other frameworks: control testing, evidence, policy generation, attestation, and reviewer-ready deliverables, with no cloud account and no vendor copy of your data. The CMMC edition is in beta.

See Axiometrik

© Sadler Enterprises LLC · Axiometrik · Not legal advice. Check your contract and your contracting officer before relying on any date or requirement here.