A BUYER'S GUIDE, NOT A SALES PITCH

DivIHN
IN SERVICE, WITH EXCELLENCE AND GRACE

The CMMC Level 1 Buyer's Guide

Choosing a Provider Without Paying for Level 2

Provider categories, fair scope,
and the questions to ask before you sign.

WHERE YOU STAND | WHO DOES WHAT | HOW TO BUY | AFTER THE ENGAGEMENT

2026

2026 CMMC FIELD MANUAL

Table of Contents

All 15requirements— 17practices— each with the wording, the assessor's questions, the artifact, Microsoft 365 and Google Workspace walkthroughs, and where small teams fail.

HOW THIS MANUAL IS ORGANISED

Before you assess — scope & count → **The 15 requirements** — the evidence for each → **Before you submit** — file & readiness → **After you submit** — keep it true

15	17 Practices	6	The evidence behind each one
Requirements		Domains	

One field manual for the CMMC Level 1 decision — requirement by requirement, evidence by evidence.

EXECUTIVE PERSPECTIVE

Level 1 Is Binary

There is areason thismanual is organised around **evidence** rather than explanation. At CMMC Level 1 there is no Plan of Action and Milestones, no grace period, and no partial credit. Every one of the requirements is either met at the moment the affirmation is signed, or the company is non-compliant. “In progress” is not a state the framework recognises.

That is what makes a field manual the right shape for the job. You do not need another document explaining why cybersecurity matters. You need to know, requirement by requirement, exactly what “met” means, the specific artifact that proves it, how to configure it in the environment you actually run — Microsoft 365 or Google Workspace — and the two or three ways small teams get it wrong. Open it at any requirement and you will find the same five-part shape.

15	17	0
FARrequirements — the obligations youmust meet, no exceptions atLevel 1.	**CMMCpractices** — the same obligations,expressed the way anassessorcounts them.	**POA&Ms allowed** — done, or not affirmed. There is no middle at Level 1.

THE FIVE-PART TREATMENT

Every requirement in Part Two follows the same shape, so you can open the manual anywhere and read it the same way.

- The requirement, in DoD wording and plain English
- The questions an assessor would ask
- The artifact that proves it — and what makes it sufficient
- Microsoft 365 and Google Workspace walkthroughs
- Where small teams fail

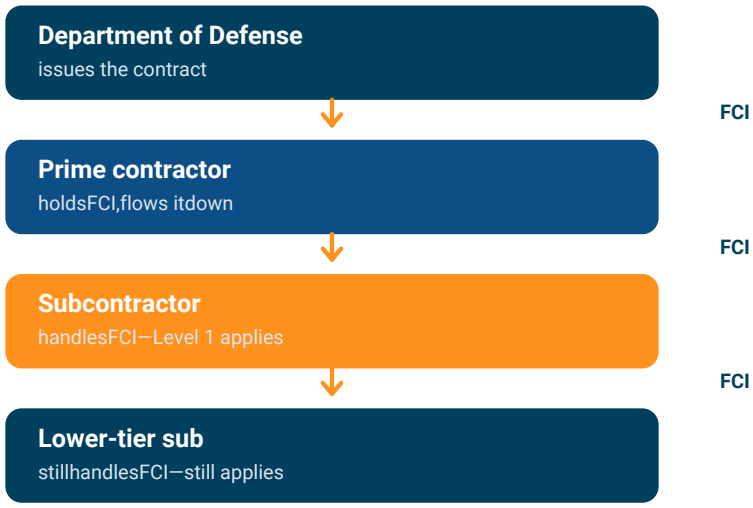
Everything that follows answers one question: can you prove it? **Not whether you do the thing — whether you can show, on the day of the assessment, the dated artifact that proves it. That is the difference between “compliant” and “affirmed.”**

BEFORE YOU ASSESS

Are You In Scope?

Level 1 appliestoany company thathandles **Federal Contract Information** — FCI — and a great many that would never call themselves defense contractors. FCI is simply information provided by or generated for the government under a contract that is not intended for public release: a shipping manifest, a facility schedule, contract correspondence, a personnel roster tied to base work. If your systems process, store or transmit any of it, Level 1 is yours to meet.

FIGURE 1 · HOW THE OBLIGATION FLOWS DOWN



Your prime's compliance does not cover you — the obligation is independently yours.

The requirement follows the FCI, not the size of the company or its distance from the government. A prime's compliance never covers its subs.

WHAT CONFIRMS IT APPLIES

- **FAR 52.204-21** in your (sub)contract — the safeguarding clause
- **DFARS 252.204-7012** signals the higher, CUI level instead
- When in doubt, ask the prime's contracts team directly

WHAT FCI IS NOT

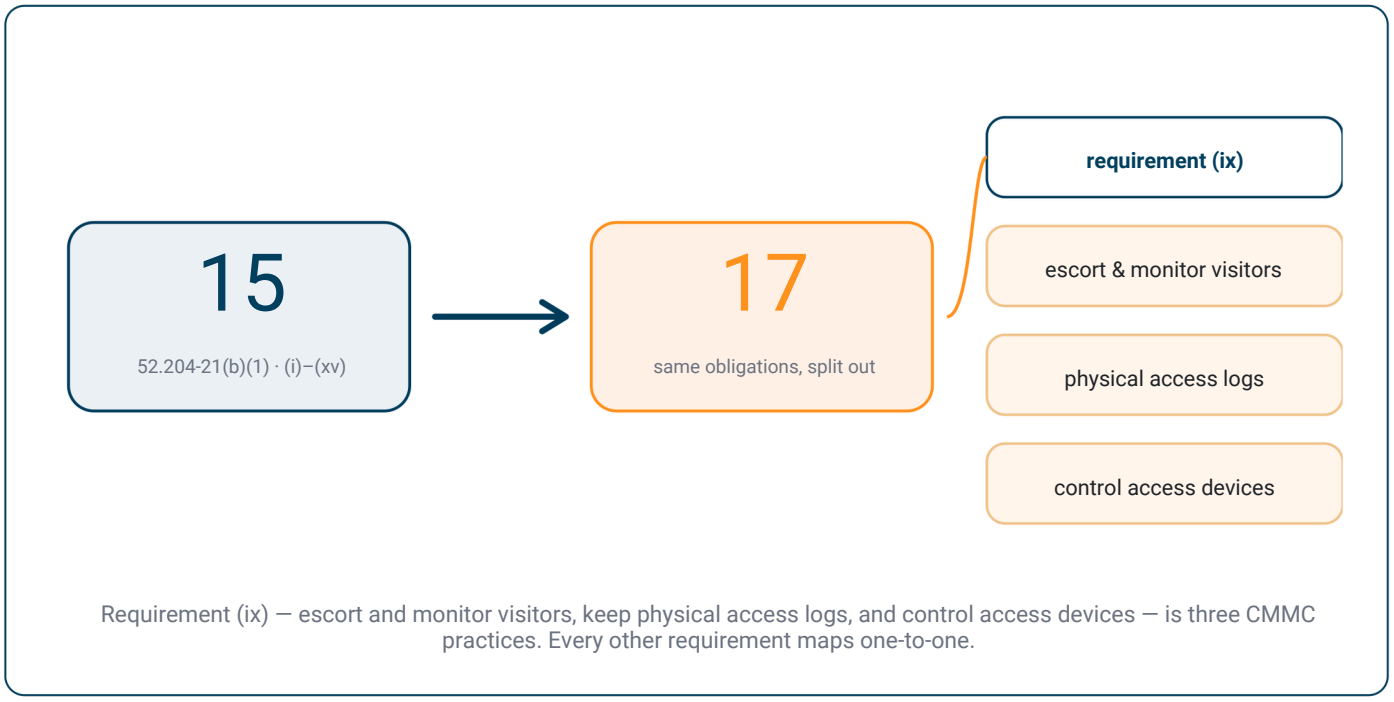
- Information already cleared for public release
- Your own internal data unrelated to a federal contract
- The same as CUI — that is Level 2 territory

BEFORE YOU ASSESS

15 Requirements or 17 Practices?

Youwill see bothnumbersinofficialmaterial,and the discrepancytrips up almost every first-time reader. They describe the **same obligations** counted two ways. FAR 52.204-21(b)(1) lists fifteen requirements, (i) through (xv). CMMC expresses them as seventeen practices, because a single requirement — (ix), on physical access — is broken into three separate practices. Nothing is added; one item is simply split.

FIGURE 2 · SAME OBLIGATIONS, TWO COUNTING CONVENTIONS



Requirement (ix) — escort and monitor visitors, keep physical access logs, and control access devices — is three CMMC practices. Every other requirement maps one-to-one.

WHY SETTLING THIS MATTERS

A manual that counts inconsistently cannot be trusted on anything. Fixing the number on page one is what earns your confidence in every requirement that follows.

ONE MORE NUMBER TO KNOW

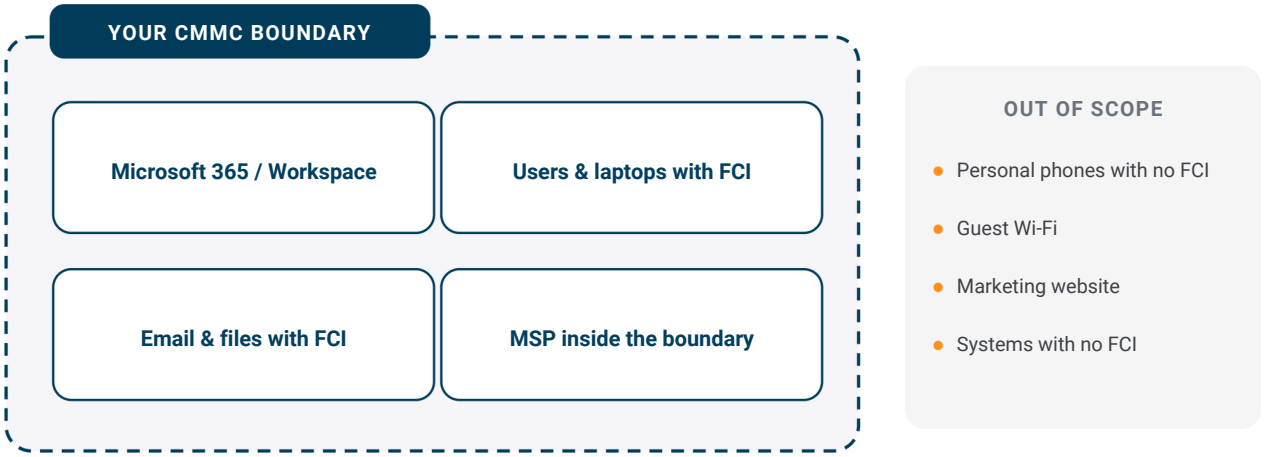
A 2026 class deviation renumbered **FAR 52.204-21** to **FAR 52.240-93**. The requirements are unchanged; both numbers still appear in solicitations, so treat them as the same clause.

BEFORE YOU ASSESS

Drawing the Boundary

Scopeis the single mostexpensivedecision a smallfirm makes at Level 1 — and the easiest to get wrong in the direction of cost. Your obligation covers only the systems that process, store or transmit FCI. Everything else is out. A ten-person firm that scopes in every laptop, mailbox, phone and provider “to be safe” can multiply its own effort several times over for no compliance benefit.

FIGURE 3 · WHAT SITS INSIDE THE BOUNDARY — AND WHAT DOES NOT



Draw the boundary tightly around FCI. External providers and MSPs that touch FCI sit inside it; systems that never see FCI stay out.

HOW EXTERNAL PROVIDERS SIT IN IT

If your MSP or a cloud service handles FCI, it is inside your boundary — and you need assurance it meets the relevant requirements. Their compliance does not become yours automatically, but their environment is part of what yours depends on.

THE CONSOLIDATION MOVE

A professional-services firm serving three primes does not need three separate programmes. One well-drawn boundary and one consolidated engagement can satisfy all of them — scope once, evidence once.

THE 15 REQUIREMENTS

Access Control

Four requirements,andthe domainthe whole assessment leans on — a gap here cascades into every other. It is about one idea in two parts: only approved people and devices get in, and once in, they can only do what their role allows.

AC.L1-3.1.1 Authorized access only

FAR (i)

In plain English: Only people, devices and processes you have approved can reach systems that hold FCI.

AN ASSESSOR ASKS

- Is there a current list of authorized users?
- Are accounts unique, and removed when people leave?

THE ARTIFACT THAT PROVES IT

An access-control policy plus a current user list, with evidence that leavers are deprovisioned promptly.

MICROSOFT 365

- Entra ID > Users: manage the authorized list
- Disable/remove accounts the day someone leaves

GOOGLE WORKSPACE

- Admin console > Directory > Users
- Suspend then delete departed users

Where small teams fail: Shared logins that no one owns; leavers whose accounts stay active for weeks; a “list” that lives only in someone’s head.

AC.L1-3.1.2 Least privilege

FAR (ii)

In plain English: Authorized users get only the access their job needs — especially administrative rights.

AN ASSESSOR ASKS

- Are admin rights limited to a named few?
- Do everyday users lack elevated privileges?

THE ARTIFACT THAT PROVES IT

A role/permission matrix and a short list of who holds admin, with the rest confirmed as standard users.

MICROSOFT 365

- Limit Global Administrators; use role-based admin
- Give staff standard, not admin, accounts

GOOGLE WORKSPACE

- Limit Super Admins; assign least-privilege roles
- Separate admin duties from daily accounts

Where small teams fail: Everyone made a local admin for convenience; several standing Global Admins; no separation between admin and daily-use accounts.

The fast path

Write one short access-control policy, export a current user list, and confirm who holds admin. Those three artifacts carry most of this domain.

The trap

Controls that exist in practice but were never written down. An assessor sees your evidence, not your habits.

ACCESS CONTROL — CONTINUED

AC.L1-3.1.20 External connections

FAR (iii)

In plain English: You verify and control how external systems and personal devices connect to yours.

AN ASSESSOR ASKS

- Are personal/BYOD devices controlled?
- Is external file sharing limited and reviewed?

THE ARTIFACT THAT PROVES IT

A policy for external connections and BYOD, plus the configured sharing and device rules that enforce it.

MICROSOFT 365

- Conditional Access: require managed/compliant devices
- SharePoint/OneDrive: restrict external sharing

GOOGLE WORKSPACE

- Context-Aware Access rules
- Drive: limit external sharing by policy

Where small teams fail: Open external sharing on everything; unmanaged personal laptops with full mailbox access; no rule at all.

AC.L1-3.1.22 Control public content

FAR (iv)

In plain English: You make sure FCI is never posted to publicly accessible systems — your website, social, public shares.

AN ASSESSOR ASKS

- Who can publish to public sites?
- Is there a review before anything goes public?

THE ARTIFACT THAT PROVES IT

A short policy naming who may post and requiring a review, with evidence the review happens.

MICROSOFT 365

- Restrict who can share files as 'anyone with the link'
- Designate an approver for public content

GOOGLE WORKSPACE

- Restrict link-sharing scope in Drive
- Designate an approver for public content

Where small teams fail: Anyone can publish to the website; a link set to 'anyone' exposes an FCI file; no review step exists.

Access Control and Identification & Authentication are the two domains to complete first — gaps here ripple into everything downstream, so they are the highest-value place to start.

The fast path

Do Access Control and Identification & Authentication together — they share the same user list and admin roster, so one export evidences both.

The trap

Treating them as separate projects and building the same evidence twice.

THE 15 REQUIREMENTS

Identification and Authentication

Tworequirements,theshortest domain —and theonesmall firms mostoftenfail, because shared and service accounts are exactly how a busy office without dedicated IT tends to operate.

IA.L1-3.5.1 Identify users & devices

FAR (v)

In plain English: Every user, process and device has its own identity — no shared or generic logins.

AN ASSESSOR ASKS

- Is every account tied to one named person?
- Are there any shared or generic accounts?

THE ARTIFACT THAT PROVES IT

A user list showing unique, named accounts, plus a device inventory — no "office@" login in daily use.

MICROSOFT 365

- One Entra account per person; avoid shared mailboxes as logins
- Register and track devices

GOOGLE WORKSPACE

- One account per person; no shared logins
- Maintain an endpoint inventory

Where small teams fail: A shared 'reception' or 'office' login used by several people; service accounts operated by humans; generic accounts no one owns.

IA.L1-3.5.2 Authenticate identities

FAR (vi)

In plain English: Identities are verified before access — in practice, strong passwords and multi-factor authentication.

AN ASSESSOR ASKS

- Are strong passwords enforced?
- Is MFA turned on for everyone?

THE ARTIFACT THAT PROVES IT

An authentication/password policy plus evidence that MFA is enabled across accounts.

MICROSOFT 365

- Enforce MFA (Conditional Access or Security Defaults)
- Set a strong password policy

GOOGLE WORKSPACE

- Enforce 2-Step Verification for all users
- Set password length/complexity requirements

Where small teams fail: MFA left off 'for now'; a shared password on a sticky note; service accounts with weak, unmanaged credentials.

> MFA is not literally spelled out in the Level 1 text, but it is the practical, defensible way to satisfy "authenticate identities" — and an assessor will expect to see it.

The fast path

Turn on MFA for everyone and remove shared logins. Those two moves, plus a user list, close almost the whole domain.

The trap

A single 'office' account everyone shares — it fails identification and authentication at once.

THE 15 REQUIREMENTS

Media Protection

Onerequirement— and theone readers most often assume is already handled. It is not about your live systems; it is about what happens to a laptop, a drive or a USB stick after it leaves your control.

MP.L1-3.8.3 Sanitize or destroy media

FAR (vii)

In plain English: Media that held FCI is wiped or destroyed before the device is disposed of, sold, donated or reassigned.

AN ASSESSOR ASKS

- How is old equipment disposed of or reused?
- Is there a record of what was wiped, and when?

THE ARTIFACT THAT PROVES IT

A media-sanitization policy and a disposal log: device, method (wipe or destroy), date, and who performed it.

MICROSOFT 365

- Remote-wipe cloud-managed devices before reissue
- Keep a certificate of destruction for drives

GOOGLE WORKSPACE

- Wipe managed ChromeOS/endpoints before reissue
- Keep a certificate of destruction for drives

Where small teams fail: A retired laptop donated without wiping; a drive repurposed between staff with data intact; USBs reused with no sanitization; no record kept.

WHAT A DEFENSIBLE DISPOSAL RECORD LOOKS LIKE

Device	Method	Date	Performed by
Laptop — asset #A-014	Full-disk wipe	2026-06-12	J. Okafor (IT)
External drive — D-3	Physically destroyed	2026-06-12	Vendor — cert #4471
USB × 4	Destroyed	2026-07-01	J. Okafor (IT)

Simple, dated, specific. A one-line entry per device is the difference between a control that is implemented and one you merely believe is.

Why this one gets skipped. **Media Protection is invisible day to day — nothing breaks when you forget it. The gap only appears the moment an assessor asks for the disposal log you never started. One shared spreadsheet, updated whenever a device leaves, closes the entire domain.**

THE 15 REQUIREMENTS

Physical Protection

Tworequirements, four practices —and thedomain small firms most often assume does not apply to them. It applies. Give it the extra attention here, especially if your workforce is remote or hybrid.

PE.L1-3.10.1 Limit physical access

FAR (viii)

In plain English: Only authorized people can physically reach the systems, equipment and areas that handle FCI.

AN ASSESSOR ASKS

- Who can physically get to FCI systems?
- How is this handled for home and remote workers?

THE ARTIFACT THAT PROVES IT

A physical-security policy and an access list; for remote staff, a signed home-office attestation.

MICROSOFT 365

- N/A at tenant level — document the physical spaces
- Lock networking/hardware; badge or key control

GOOGLE WORKSPACE

- N/A at tenant level — document the physical spaces
- Lock networking/hardware; badge or key control

Where small teams fail: An unlocked office anyone can enter; a router and NAS on an open shelf; remote workers' home offices ignored entirely.

PE.L1-3.10.3 Escort & monitor visitors

FAR (ix)a

In plain English: Visitors to areas with FCI systems are escorted and their activity is monitored.

AN ASSESSOR ASKS

- Are visitors escorted, not left alone?
- Is visitor activity actually watched?

THE ARTIFACT THAT PROVES IT

A visitor policy plus a visitor log that records the escort.

MICROSOFT 365

- Not a tenant setting — a documented office practice
- —

GOOGLE WORKSPACE

- Not a tenant setting — a documented office practice
- —

Where small teams fail: Visitors buzzed in and left to roam; no escort for contractors near FCI systems; a policy that exists but is never followed.

The fast path

Write a one-page physical-security policy and a home-office attestation, then start a simple visitor and key log. Most of PE is documentation, not technology.

The trap

Assuming a cloud-first or remote firm is exempt. Physical protection still applies — it just moves into the home office.

PHYSICAL PROTECTION — CONTINUED

PE.L1-3.10.4 Physical access logs

FAR (ix)b

In plain English: You keep a record of who physically entered areas with FCI systems.

AN ASSESSOR ASKS

- Is there a log of physical entry?
- Is it kept and reviewable?

THE ARTIFACT THAT PROVES IT

A visitor/access log — a sign-in sheet or electronic record — retained over time.

MICROSOFT 365

- Not a tenant setting — keep a sign-in record
- —

GOOGLE WORKSPACE

- Not a tenant setting — keep a sign-in record
- —

Where small teams fail: No log at all; a log started and abandoned; entries with no date or name.

PE.L1-3.10.5 Control access devices

FAR (ix)c

In plain English: Keys, badges and other physical access devices are tracked, issued and recovered.

AN ASSESSOR ASKS

- Are keys/badges inventoried?
- Are they recovered when someone leaves?

THE ARTIFACT THAT PROVES IT

A key/badge inventory and an issue-and-return log tied to onboarding and offboarding.

MICROSOFT 365

- Not a tenant setting — keep a key/badge register
- —

GOOGLE WORKSPACE

- Not a tenant setting — keep a key/badge register
- —

Where small teams fail: Keys handed out and never tracked; a departed employee who still has a working badge; no inventory exists.

The home-office question, answered. **A remote or hybrid workforce does not exempt you from Physical Protection — it distributes it. The practical answer is a short home-office policy plus a signed attestation from each remote worker: FCI devices are kept in a controlled space, screens are not left exposed, and household members do not use the work device. Competitors avoid this question; do not.**

The fast path

Three short documents — a physical-security policy, a home-office attestation, and a combined visitor-and-key log — evidence all four Physical Protection practices at once.

The trap

A register or attestation created once and never kept current. A stale log reads as no log at all to an assessor.

THE 15 REQUIREMENTS

System and Communications Protection

Tworequirements—and thedomainwhose vocabulary isfurthestfromasmallfirm'sdaily experience. "Boundary" sounds like a data-centre word. Translated: it means the edge of your environment, which for most small firms is a cloud tenant and a handful of laptops.

SC.L1-3.13.1 Boundary protection

FAR (x)

In plain English: You monitor, control and protect communications at the edge of your environment.

AN ASSESSOR ASKS

- What protects the edge of your network?
- In the cloud, what controls the tenant boundary?

THE ARTIFACT THAT PROVES IT

Firewall configuration and, for cloud, the tenant security settings that govern access in and out; a simple network diagram.

MICROSOFT 365

- Defender + Exchange Online Protection as the boundary
- Conditional Access as the tenant edge control

GOOGLE WORKSPACE

- Google's built-in spam/malware protection
- Context-Aware Access as the tenant edge control

Where small teams fail: No firewall on the office network; open remote-desktop to the internet; assuming "we're in the cloud, so there's no boundary."

SC.L1-3.13.5 Separate public components

FAR (xi)

In plain English: Publicly accessible components are separated from your internal, FCI-handling systems.

AN ASSESSOR ASKS

- Is your public website separated from internal systems?
- Are any public services on the internal network?

THE ARTIFACT THAT PROVES IT

A network diagram showing separation, and the hosting arrangement that keeps public services off your internal LAN.

MICROSOFT 365

- Host the public website away from the tenant
- Keep no public-facing service on internal systems

GOOGLE WORKSPACE

- Host the public website away from the tenant
- Keep no public-facing service on internal systems

Where small teams fail: A public web server sitting on the internal office network; a shared box serving both public and internal roles.

The fast path

Screenshot your tenant security settings and draw a one-page network diagram. For a cloud-and-laptops firm, that is the boundary.

The trap

Reading 'boundary' as a data-centre term and concluding it does not apply. It does — your tenant is the boundary.

THE 15 REQUIREMENTS

System and Information Integrity

Fourrequirements—the largest domain bycount, and the easiesttoevidence,because the tools that satisfy it are almost certainly already running. Say it plainly: this is your early win.

SI.L1-3.14.1 Flaw remediation

FAR (xii)

In plain English: System and application flaws are identified and corrected in a timely way — in short, you patch.

AN ASSESSOR ASKS

- Are OS and apps updated promptly?
- Is there evidence they are current?

THE ARTIFACT THAT PROVES IT

An update policy plus reports or screenshots showing devices are patched and current.

MICROSOFT 365

- Windows Update / Intune update rings
- Keep Office apps on a supported, updating channel

GOOGLE WORKSPACE

- ChromeOS auto-update; managed browser updates
- Endpoint patching via your device management

Where small teams fail: Updates set to manual and forgotten; an unsupported OS still in use; no evidence of patch status.

SI.L1-3.14.2 Malicious-code protection

FAR (xiii)

In plain English: Anti-malware protection is in place on the systems that handle FCI — on every device.

AN ASSESSOR ASKS

- Is antivirus on all endpoints?
- Any device missing coverage?

THE ARTIFACT THAT PROVES IT

An anti-malware policy and a deployment report showing every in-scope endpoint is protected.

MICROSOFT 365

- Microsoft Defender Antivirus on all endpoints
- Defender for Office 365 on email

GOOGLE WORKSPACE

- Deploy endpoint AV (Defender or third-party)
- Gmail's built-in malware scanning

Where small teams fail: Antivirus on most machines but not all — the single most common Level 1 gap; a personal laptop with none.

The fast path

Confirm updates and antivirus are on across every device, then capture the reports. The tooling is usually already there.

The trap

One unmanaged laptop with no antivirus — the single most common Level 1 finding, and an easy one to miss.

SYSTEM AND INFORMATION INTEGRITY — CONTINUED

SI.L1-3.14.4 Update protection mechanisms

FAR (xiv)

In plain English: Your malicious-code protection updates itself as new definitions and releases become available.

AN ASSESSOR ASKS

- Do AV definitions update automatically?
- Are they current across all devices?

THE ARTIFACT THAT PROVES IT

Antivirus configuration showing automatic updates enabled, with recent definition dates.

MICROSOFT 365

- Defender definitions auto-update by default — confirm it
- Verify no device is excluded

GOOGLE WORKSPACE

- Confirm endpoint AV auto-updates
- Verify no device is excluded

Where small teams fail: Definitions weeks out of date; auto-update disabled on a machine; one excluded device quietly unprotected.

SI.L1-3.14.5 System & file scanning

FAR (xv)

In plain English: You run periodic scans of systems and real-time scans of files from external sources.

AN ASSESSOR ASKS

- Are scheduled scans configured?
- Is real-time protection on for downloads and email?

THE ARTIFACT THAT PROVES IT

Antivirus configuration showing scheduled and real-time scanning, plus email-attachment scanning.

MICROSOFT 365

- Defender: scheduled + real-time scans on
- Safe Attachments scanning on email

GOOGLE WORKSPACE

- Endpoint AV: scheduled + real-time on
- Gmail attachment scanning on

Where small teams fail: Real-time protection switched off; no scheduled scan; downloads and attachments never scanned.

Take the early win. **If Defender or an equivalent is already deployed and updating — and for most Microsoft 365 and Workspace shops it is — four of your seventeen practices are largely evidenced already. Capture the screenshots, note the coverage, and move on.**

The fast path

Open Defender once and screenshot the update and scan settings — a single capture evidences both SI.L1-3.14.4 and SI.L1-3.14.5. Then confirm no device is excluded.

The trap

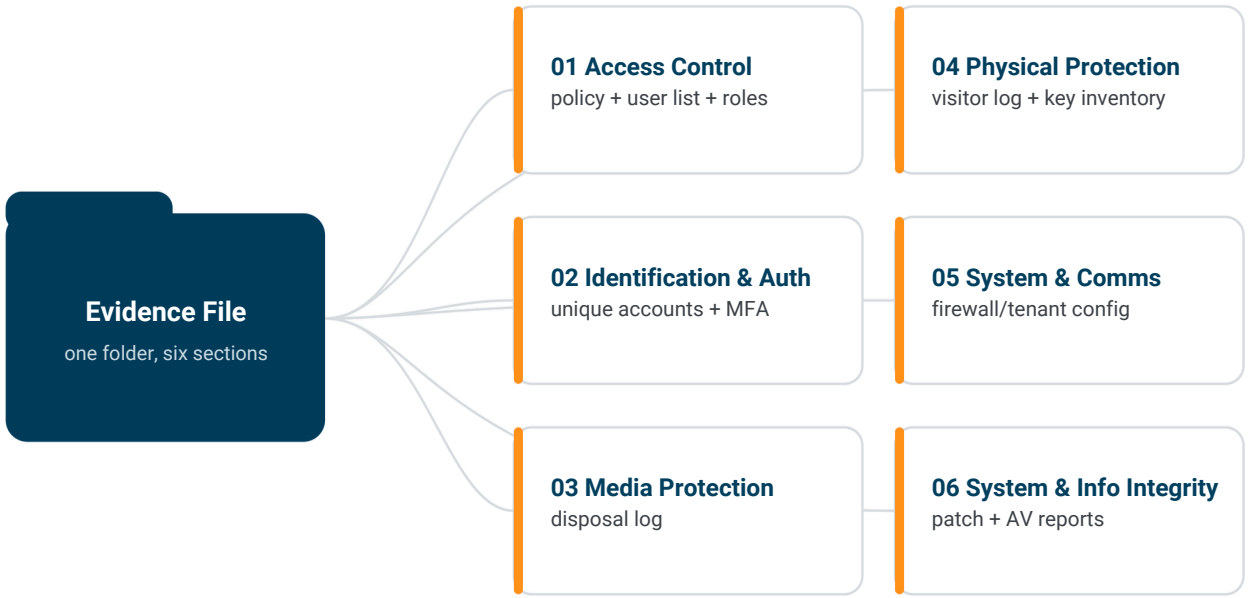
Assuming “on by default” equals “evidenced.” The assessor wants the screenshot with a recent definition date, not your word that it updates.

BEFORE YOU SUBMIT

Building the Evidence File

Nine domain chapters produceonedeliverable:a single, organised evidence file that a contracting officer — or your own affirming official — can open and follow. The work is not just having the controls; it is being able to show them, quickly, in a structure that mirrors the requirements themselves.

FIGURE 4 · ONE FOLDER, SIX SECTIONS, EVERY ARTIFACT IN ITS PLACE



Structure the file by domain, name each artifact for the practice it satisfies, and date everything. A stranger should be able to navigate it without you.

MAKE EACH ARTIFACT COUNT

- Name it for the practice ID it proves
- Date it — when it was captured or last verified
- Attribute it — who produced or confirmed it
- Keep it current between affirmations

SUFFICIENT, NOT SUGGESTIVE

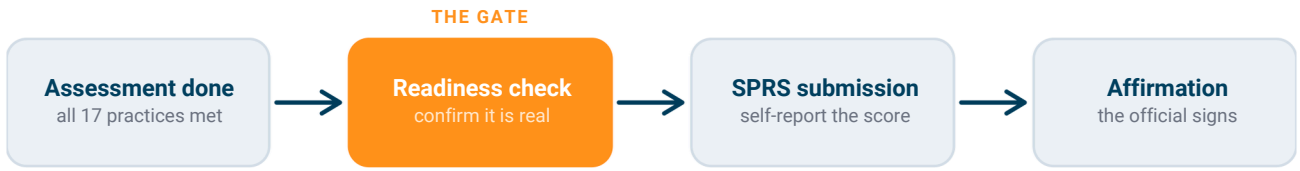
A screenshot of a setting is evidence; a claim that “we do that” is not. The test for each artifact is simple: would it satisfy an assessor who had never met you and assumed nothing?

BEFORE YOU SUBMIT

The Readiness Check

Beforeanyoneopens SPRS,onegate. Thereadinesscheck is not the assessment repeated — it is the short, honest confirmation that the assessment is genuinely complete, the evidence genuinely exists, and the score you are about to report genuinely matches reality. It is the last moment to find a gap while it is still free to fix.

FIGURE 5 · WHERE THE GATE SITS



One checkpoint between finishing the work and reporting it — cheap to pass when the evidence is real, expensive to skip.

WHAT MUST BE TRUE BEFORE SPRS

- All 17 practices are implemented — not “nearly”
- Every practice has a sufficient, dated artifact
- Antivirus coverage is confirmed on every device
- Access-control policy is written, not just practised
- Removable media handling is documented
- The evidence file is organised and findable
- The self-reported score matches the assessment
- Scope is confirmed — nothing assumed in or out

THE THREE RECURRING GAPS

- Antivirus missing on some devices
- Access control done in practice but never written down
- USB / removable media with no sanitization step

THEN, THE SIGNATURE

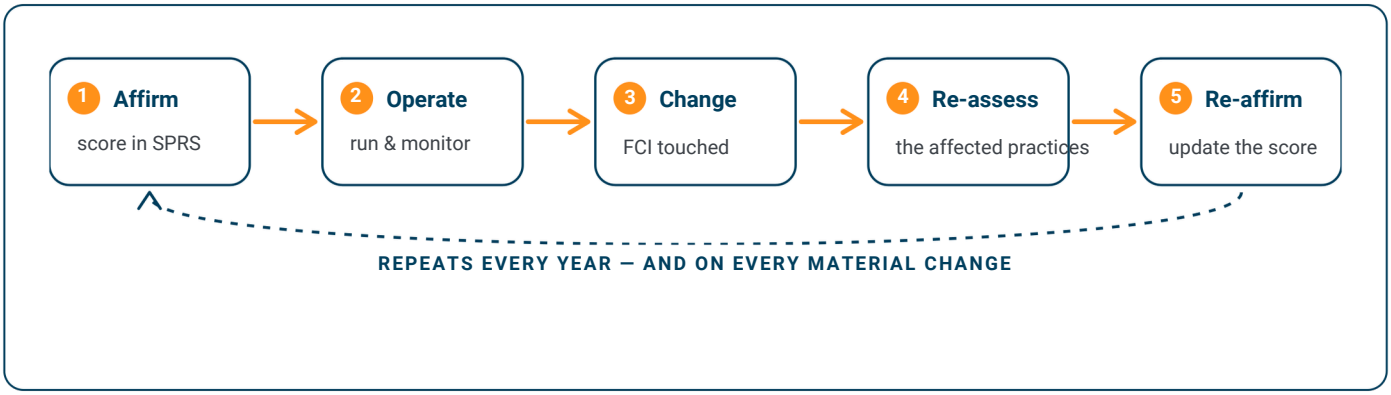
The readiness check ends at the edge of the affirmation itself. Who signs, what they are attesting to, and the personal weight it carries are the subject of the companion guide, **Signing the Affirmation**.

AFTER YOU SUBMIT

When the Environment Changes

Level1is annual,butcompliance is continuous.The affirmation describes your environment at a moment; the business keeps moving, and some ordinary changes quietly take you out of the state you affirmed. The discipline is not to re-do everything constantly — it is to recognise the handful of changes that oblige a fresh look, and to act on them when they happen rather than at renewal.

FIGURE 6 · THE CONTINUOUS COMPLIANCE LOOP



WHAT TRIGGERS A MID-YEAR REASSESSMENT

A new cloud service

A tool that starts handling FCI joins your boundary — and your assessment.

A new contract

New FCI, or a step up toward CUI, can change scope or even your level.

A headcount change

New hires need provisioning; leavers need deprovisioning and key recovery.

A new system or app

Anything that touches FCI is in scope the day it goes live.

WHAT TO DO ABOUT IT

- Re-assess only the affected practices
- Refresh the evidence for what changed
- Update the score if implementation moved

MAKE IT ROUTINE

Add one line to your change process: “does this touch FCI?” If yes, it touches your assessment — and someone should own the answer before the change ships.

APPENDIX

Evidence Index: All 17 Practices

Thewholemanualonone page — every practice, itsartifact,andthechapter that covers it. This is the page to print, share internally, and pass down a supply chain. It stands alone.

Practice	Requirement	Artifact	Ch.
AC.L1-3.1.1	Authorized access only	Access policy + current user list	4
AC.L1-3.1.2	Least privilege	Role/permission matrix + admin list	4
AC.L1-3.1.20	External connections	BYOD/external policy + sharing rules	4
AC.L1-3.1.22	Control public content	Public-posting policy + review record	4
IA.L1-3.5.1	Identify users & devices	Unique-account list + device inventory	5
IA.L1-3.5.2	Authenticate identities	Password policy + MFA evidence	5
MP.L1-3.8.3	Sanitize or destroy media	Disposal policy + dated disposal log	6
PE.L1-3.10.1	Limit physical access	Physical policy + home-office attestation	7
PE.L1-3.10.3	Escort & monitor visitors	Visitor policy + escorted visitor log	7
PE.L1-3.10.4	Physical access logs	Retained physical access log	7
PE.L1-3.10.5	Control access devices	Key/badge inventory + issue-return log	7
SC.L1-3.13.1	Boundary protection	Firewall/tenant config + network diagram	8
SC.L1-3.13.5	Separate public components	Network diagram + hosting arrangement	8
SI.L1-3.14.1	Flaw remediation	Update policy + patch-status evidence	9
SI.L1-3.14.2	Malicious-code protection	AV policy + full-coverage report	9
SI.L1-3.14.4	Update protection mechanisms	AV auto-update config + definition dates	9
SI.L1-3.14.5	System & file scanning	AV scan config + email scanning	9

A working version of this index — the **Evidence Tracker (Excel)** — accompanies this manual.

REFERENCE

CMMC Level 1 Glossary

Thevocabularythismanualuses,inplainterms—enoughto work every requirement without stopping to look things up.

CMMC
Cybersecurity Maturity Model Certification — the DoD programme verifying contractor cybersecurity.

Level 1
Thefoundational tier — basic safeguarding of FCI; self-assessed; no POA&Ms.

FCI
Federal Contract Information — non-public information provided or generated under a federal contract.

CUI
Controlled Unclassified Information — protected at Level 2, not Level 1.

Practice
AsingleCMMC control; Level 1 has 17.

Requirement
AFAR52.204-21(b)(1) item; there are 15, mapping to 17 practices.

FAR 52.204-21
Thesafeguardingclause behind Level 1 (renumbered 52.240-93 in 2026).

Domain
Agrouping of practices — AC, IA, MP, PE, SC, SI.

Ar tifact
Theconcrete evidence that proves a practice is met.

SPRS
Supplier Performance Risk System — where the self-assessment score is recorded.

Self-assessment
Yourownevaluation against the 17 practices, submitted to SPRS.

Affirmation
Thesigned statement that the requirements are met (see the companion guide).

POA&M
Plan ofAction & Milestones — allowed at higher levels, not at Level 1.

MFA / 2SV
Multi-factor/2-Step Verification — the practical way to satisfy authentication.

Boundary
The edgeof your in-scope environment — often a cloud tenant plus laptops.

Scope
Thesystems that process, store or transmit FCI — and only those.

MSP
Managed Service Provider — if it touches FCI, it is inside your boundary.

Flow-down
How therequirement passes from prime to subcontractor with the FCI.

Prime / Sub
Thecontractor holding the DoD contract, and those working under it.

Sanitize
Wipeor destroy media so FCI cannot be recovered before disposal or reuse.

REFERENCE

About DivIHN

DivIHNisaCMMC Level2certifiedorganisation, and Level 2-experienced practitioners lead every Level 1 engagement. We help small DoD contractors and subs meet Level 1 the way this manual describes it — scoped tightly, evidenced properly, and documented so it holds up when someone asks.

HOW WE HELP

Scoping & gap assessment

Drawing the boundary and finding the gaps before an assessor does.

Evidence & remediation

Building the dated evidence file, practice by practice.

Scope-change & renewal support

Keeping the file current as the environment moves.

SOURCES & COMPANIONS

- FAR 52.204-21 (renumbered 52.240-93, 2026) · NIST SP 800-171
- DivIHN — What CMMC Means for DoD Subcontractors
- DivIHN — How to Complete Your CMMC Level 1 Self-Assessment
- Companion ebook — Signing the Affirmation
- Companion tool — the Evidence Tracker (Excel)

Note on numbers. Practice IDs and clause citations follow current CMMC and FAR references; confirm the version cited in your specific solicitation, as both the 52.204-21 and 52.240-93 numbers remain in circulation.

Working through Level 1?

Talkto DivIHNaboutscopingtightlyandbuildingtheevidence file that makes your affirmation defensible.

- divihn.com/cmmc
- CMMC Practice