greypike

CMMC SCOPING SERIES · WORKBOOK 01

CUI Boundary Workbook

The comprehensive guide to defining your CMMC Level 2 scope.

Scope first. Then controls.

CMMC LEVEL 2 · 15 PAGES · FILLABLE

WHY THIS WORKBOOK EXISTS

Most contractors approach CMMC compliance backwards. They secure everything first, then figure out what's in scope. The result: inflated assessment costs, sprawling documentation, and ongoing compliance burden on systems that never touched CUI in the first place.

This workbook walks you through the opposite approach — with tips, common pitfalls, worked examples, and the reference material you need to defend your scope to an assessor.

WHAT'S INSIDE

FOUR PRINCIPLES

1. Smaller is better.

Every system, user, and process inside your boundary is something you must secure, document, monitor, and defend. Reduce first.

2. CUI defines the boundary — not the other way around.

Start by finding where CUI lives and flows. The boundary is the consequence of that reality, not a line you draw first.

3. Segmentation is not optional.

If out-of-scope systems can reach in-scope systems without meaningful controls, they are in scope. Segment with intent.

4. Document the 'why'.

Assessors don't just want a boundary — they want the reasoning. Why is this system in? Why is that one out? Write it down as you go.

TIP **Scope is the single biggest lever on your cost.**

Every asset you add to scope multiplies your documentation, monitoring, and assessment burden. Contractors who reduce scope by 50% routinely cut their first-year CMMC cost by more than that.

AVOID **Don't scope the company — scope the CUI.**

The most expensive mistake we see: treating every laptop, server, and user as in-scope 'to be safe.' CMMC is about protecting CUI in a defined place, not about securing the entire business to government standards.

YOUR WORKING DEFINITION OF CUI

Before inventorying anything, write a one-paragraph definition of the CUI your organization actually handles. Reference the contract(s), the CUI category, and the specific types of data (drawings, specifications, technical reports, etc.). This becomes your reference point for every scoping decision that follows.

CONTRACT(S) THAT TRIGGER CMMC

PRIMARY CONTRACT / PROGRAM

CONTRACTING AGENCY

CMMC LEVEL REQUIRED

ASSESSMENT TARGET DATE

TIP **Check the DoD CUI Registry.**

The CUI Registry (dodcui.mil) lists every official CUI category. If your data doesn't fit a registered category, it may not actually be CUI — and that changes your scope dramatically. When in doubt, ask the contracting officer.

AVOID **FCI is not CUI — don't confuse the two.**

Federal Contract Information (FCI) requires CMMC Level 1. CUI requires Level 2. Marking FCI as CUI inflates your scope unnecessarily; marking CUI as FCI leaves you under-protected and non-compliant.

CMMC Level 2 recognizes five asset categories. Getting this right is the foundation of a defensible scope — the category determines what controls apply and what evidence you need to collect.

CATEGORY	WHAT IT IS	ASSESSMENT TREATMENT
CUI Asset	Processes, stores, or transmits CUI.	Fully in scope. All 110 Level 2 controls apply. Full documentation and assessment required.
Security Protection Asset (SPA)	Provides security to CUI assets (firewalls, SIEM, IAM, EDR, backup).	In scope for the controls they provide. Assessed against the specific capabilities they deliver to the CUI environment.
Contractor Risk Managed Asset (CRMA)	Can access CUI but is managed so that it shouldn't, e.g. general-purpose laptops with policy restrictions.	Partial scope. Documented in SSP; assessed for policy and physical/logical protections — not against all 110 controls.
Specialized Asset	Equipment that may process CUI but isn't a general-purpose IT system (IoT, OT, test equipment, GFE).	Documented in SSP and listed on network diagrams. Managed via risk-based approach, not full control set.
Out-of-Scope Asset	Cannot access CUI and is physically/logically separated from the CUI environment.	Not assessed. Must be demonstrably separated — segmentation evidence required.

TIP **CRMA is the most powerful scope-reduction tool — when used honestly.**

Properly-implemented CRMAs let you keep general-purpose endpoints out of full scope. But assessors look hard at this. You need real policy, real enforcement, and a credible reason those endpoints won't handle CUI.

AVOID **Don't call something 'Specialized' just to avoid controls.**

Specialized Assets exist for genuinely unusual equipment — test rigs, OT, legacy GFE. Standard Windows servers don't qualify. Misclassification is one of the fastest ways to fail an assessment.

List every location where CUI is received, created, stored, processed, or transmitted. Include email, file shares, engineering systems, cloud services, endpoints, removable media, and physical locations. If you're not sure whether something holds CUI, list it — you'll confirm it later.

LOCATION / SYSTEM	TYPE OF CUI	HOW IT ARRIVES	WHERE IT RESTS	OWNER

TIP **Follow the data, not the org chart.**

Trace at least one real contract deliverable from receipt to delivery. Every place it touches — email, laptop, file share, print queue, vendor portal — is a location that belongs in this inventory.

This is how a small defense contractor (10-person engineering firm, one CUI contract) might fill out the inventory. Use it as a reference for detail level and categorization — not as a template to copy.

LOCATION / SYSTEM	TYPE OF CUI	HOW IT ARRIVES	WHERE IT RESTS	OWNER
DoD SAFE inbox	Tech drawings (CUI//SP-PROP)	Customer upload link	Downloaded to enclave file share	Eng. lead
Enclave SharePoint	Drawings, specs, reports	From SAFE + created internally	Cloud (US-only)	IT
Enclave laptops (×3)	Working copies of drawings	SharePoint sync	Encrypted local drive	Eng. team
Encrypted email	Status updates referencing CUI	Sent/received via enclave M365	Mailbox + archive	Program mgr
Shop floor print station	Printed drawings for fabrication	Print job from enclave laptop	Locked cabinet post-use	Shop lead
Subcontractor (Machine Shop X)	Subset of drawings	Encrypted file transfer	Their CUI enclave	PM + sub PM

EXAMPLE **What makes this inventory strong**

- Specific systems — not 'our file share' but 'Enclave SharePoint.'
- CUI category noted where known (SP-PROP = Proprietary Business Info).
- Physical locations counted (print station, locked cabinet).
- Every subcontractor who touches CUI is listed with an internal owner.

AVOID **Don't stop at 'email' — name the mailbox, name the system.**

Assessors probe vague entries. 'Email' is not an inventory entry; 'Enclave M365 mailboxes for Alice, Bob, and Carol' is. Specificity is what separates a defensible scope from a checkbox exercise.

Draw your proposed CUI enclave boundary. Indicate what systems, networks, and users sit inside it, and what connections cross it. A clear sketch that an assessor could understand is enough — it doesn't have to be a formal network diagram.

Sketch your boundary here — print and draw, or annotate digitally

BOUNDARY DESCRIPTION

TIP **Label every line that crosses the boundary.**

Every ingress and egress point should have a purpose attached to it (email gateway, customer file transfer, vendor VPN). Unlabeled arrows are questions an assessor will ask — answer them preemptively.

List every asset and person inside the boundary. Use the five categories from Page 4 to classify each asset — this classification drives which controls apply.

ASSETS

ASSET NAME / HOSTNAME	CATEGORY	LOCATION	OWNER

PEOPLE WITH CUI ACCESS

NAME	ROLE	ACCESS REASON	ACCESS METHOD

AVOID **Admins and IT staff count as 'people with CUI access.'**

Anyone who can read, copy, or restore CUI — including IT admins, MSP techs, and backup operators — is in scope. Omitting them is one of the most common reasons scoping documentation fails its first review.

Describe the technical controls that keep out-of-scope systems from reaching the CUI enclave (and vice versa). Assessors will push on this — weak segmentation is the fastest way to pull your entire environment into scope.

SEGMENTATION CONTROLS IN PLACE

- ☐ Network segmentation (VLANs, subnets, firewalls)
- ☐ Identity boundary (separate directory, tenant, or group structure)
- ☐ Dedicated endpoints for CUI work
- ☐ Encrypted transmission across the boundary
- ☐ Data loss prevention / egress controls
- ☐ Physical access controls for CUI locations

DESCRIBE EACH CONTROL IN ONE OR TWO SENTENCES

AUTHORIZED FLOWS CROSSING THE BOUNDARY

AVOID **Shared IT services break boundaries quietly.**

Shared identity (one Azure AD/Entra tenant for CUI and non-CUI users), shared backup, and shared logging are the three most common reasons an 'enclave' ends up functionally merged with the rest of the business.

DFARS 252.204-7012 requires flow-down of CUI protection requirements to any subcontractor handling your CUI. Map them here. Each sub must have appropriate CMMC status or equivalent protections — and you are responsible for verifying it.

SUBCONTRACTOR	CUI RECEIVED	TRANSFER METHOD	CMMC STATUS	VERIFIED

External services that touch CUI

Cloud services, MSPs, ESPs, and vendors with access to your enclave.

SERVICE / VENDOR	ROLE	FEDRAMP / CMMC	ACCESS SCOPE

TIP **External Service Providers (ESPs) inherit your scope.**

If an ESP (MSP, SaaS, cloud) processes, stores, or transmits your CUI — or provides security services that protect CUI — they are in scope for CMMC. Get their Customer Responsibility Matrix (CRM) or equivalent in writing.

AVOID **Commercial Microsoft 365 and commercial Google Workspace are not CUI-ready.**

CUI requires FedRAMP Moderate or High equivalence — which in practice means GCC High, a FedRAMP-authorized enclave, or an equivalent dedicated environment. Commercial tenants fail this bar regardless of how they're configured.

These are the patterns we see most often in contractors who are about to fail an assessment — or about to spend two to three times what they needed to. Work through each one against your own environment.

- × **“Everything is in scope — we're just being safe.”**
  The most expensive mistake in CMMC. Securing everything to Level 2 standards is rarely cheaper than segmenting — and it's almost never faster.
- × **“Our MSP handles security, so we're fine.”**
  Unless your MSP has CMMC Level 2 status or is itself in a verified CUI enclave, they are a liability, not a solution. Their access to your systems is in scope for your assessment.
- × **“We use M365 — Microsoft is FedRAMP.”**
  Commercial M365 is not GCC High. The commercial cloud is not approved for CUI regardless of how hardened your tenant is. This is a binary rule, not a configuration question.
- × **“We'll just encrypt CUI and leave it in our main environment.”**
  Encryption addresses confidentiality at rest. It does not address logging, access control, personnel security, physical controls, or the other 100+ requirements in Level 2.
- × **“Our IT admins don't look at CUI, so they're not in scope.”**
  Privileged access is access. If an admin can read, copy, restore, or modify CUI systems, they are in scope regardless of whether they ‘actually look.’
- × **“The subcontractor is small — flow-down doesn't really apply.”**
  DFARS flow-down applies regardless of size. If they touch your CUI, you are on the hook for verifying their compliance posture.

Walk through this checklist before finalizing scope. Any unchecked item is a scoping risk — either resolve it or document why it's acceptable.

CUI IDENTIFICATION

- [ ] I have a written definition of the CUI we handle.
- [ ] Every contract requiring CMMC has been reviewed.
- [ ] CUI categories confirmed against the DoD CUI Registry.

BOUNDARY COMPLETENESS

- [ ] Every location from the CUI inventory is inside the boundary.
- [ ] Nothing inside the boundary lacks a documented reason to be there.
- [ ] The boundary is documented both visually and in writing.
- [ ] Every asset is classified (CUI Asset, SPA, CRMA, Specialized, Out-of-scope).

SEGMENTATION INTEGRITY

- [ ] Out-of-scope users cannot reach in-scope systems without authorization.
- [ ] Out-of-scope systems cannot initiate connections to in-scope systems.
- [ ] All authorized cross-boundary flows are explicitly listed.
- [ ] Shared services (IAM, logging, backup) are handled as SPAs with appropriate controls.

THIRD PARTIES

- [ ] Every vendor, MSP, or ESP with access to the enclave is documented.
- [ ] Each has appropriate CMMC or FedRAMP status — and we have evidence.
- [ ] DFARS flow-down is verified for every CUI-handling subcontractor.

READY FOR ASSESSMENT

- [ ] Scope has been reviewed with a qualified assessor or advisor.
- [ ] Scope reduction opportunities have been explored, not just accepted as-is.

Scope is the foundation. Once it's settled, these are the pieces you still need in place before a C3PAO shows up. Treat this as a gate — if you can't check it, don't book the assessment.

Documentation readiness

- [ ] System Security Plan (SSP) covers the full defined scope.
- [ ] POA&M tracks every not-yet-met control with owner and target date.
- [ ] Policy library covers all 14 Level 2 domains.
- [ ] Network diagram matches the current boundary.
- [ ] Data flow diagram shows CUI in motion across the boundary.
- [ ] Customer Responsibility Matrix obtained from every ESP/cloud provider.

Operational evidence

- [ ] Access reviews completed within the last quarter.
- [ ] Audit logs retained and searchable across the boundary (typically 90+ days).
- [ ] Vulnerability scanning running on a regular cadence with remediation tracking.
- [ ] Incident response plan tested — tabletop within the last 12 months.
- [ ] Security awareness training completed by all in-scope personnel.
- [ ] Backups tested; restoration procedure documented.

Questions the assessor will ask

- “Walk me through how CUI enters your environment.”
- “Show me where this specific piece of CUI is right now.”
- “Who has access to the CUI enclave, and how is that list maintained?”
- “How do you know an out-of-scope system can't reach an in-scope system?”
- “When was the last time you reviewed this?”

TIP **Rehearse the first five minutes of the assessment.**

Your opening walkthrough sets the tone. Pick one CUI item, walk it end-to-end (ingress → storage → use → disposition), and name the controls protecting it at each stage. If your team can do this cleanly, the rest tends to follow.

The scope defined in this workbook has been reviewed and is approved as the basis for subsequent CMMC activities (SSP, POA&M, and assessment preparation).

APPROVALS

PREPARED BY

Name	Signature	Date

REVIEWED BY (SECURITY LEAD)

Name	Signature	Date

APPROVED BY (EXECUTIVE SPONSOR)

Name	Signature	Date

REVISION HISTORY

VERSION	DATE	AUTHOR	SUMMARY OF CHANGES

Quick reference for the acronyms and terms used throughout this workbook and throughout the CMMC assessment process.

C3PAO	CMMC Third-Party Assessor Organization. The only entities authorized to conduct Level 2 certification assessments.
CMMC	Cybersecurity Maturity Model Certification. DoD's framework for verifying contractor cybersecurity.
CRM	Customer Responsibility Matrix. Document from a cloud provider or ESP showing which controls they provide vs. those the customer owns.
CRMA	Contractor Risk Managed Asset. Asset that can access CUI but is managed with policy and protections to limit that access.
CUI	Controlled Unclassified Information. Government-owned information that requires safeguarding but is not classified.
DFARS	Defense Federal Acquisition Regulation Supplement. DFARS 252.204-7012 governs CUI safeguarding.
DIB	Defense Industrial Base. The network of contractors and subcontractors that support the DoD.
Enclave	A dedicated, segmented environment used to handle CUI, separated from the rest of a contractor's IT.
ESP	External Service Provider. Any third party providing IT or security services that process, store, or transmit CUI, or protect assets that do.
FCI	Federal Contract Information. Requires CMMC Level 1 — a lower bar than CUI.
FedRAMP	Federal Risk and Authorization Management Program. Standardized security assessment for cloud services used by the federal government.
GCC High	Government Community Cloud High. Microsoft's FedRAMP High-authorized government cloud offering for CUI.
POA&M	Plan of Action & Milestones. Tracks controls not yet fully met, with owners and target dates.
RPA / RPO	Registered Practitioner / Registered Practitioner Organization. Individuals and firms credentialed to advise on CMMC.
SPA	Security Protection Asset. System or service that provides security to CUI assets (firewalls, SIEM, IAM, etc.).
SPRS	Supplier Performance Risk System. Where contractors report their self-assessment score.
SSP	System Security Plan. The core document describing your CUI environment and the controls protecting it.