THE COMPLETE

CMMC ROADMAP

FOR DEFENSE CONTRACTORS

A practical guide to achieving CMMC compliance and preparing for assessment success.

IRONSTACK

2026 DEFENSE CONTRACTOR EDITION

CMMC Roadmap & Readiness Checklist

A practical workbook to identify CMMC gaps, define your assessment boundary, organize evidence, and turn compliance uncertainty into a clear action plan.

- Readiness scoring
- Boundary worksheet
- Evidence tracker
- 90-day sprint plan

Prepared for organizations pursuing CMMC readiness and assessment preparation.

START HERE

Use this workbook to find your next best compliance move.

01

CMMC readiness is not just a control checklist. It is a sequence of decisions: what information you handle, where it flows, which systems are in scope, which controls are implemented, and what evidence proves they operate.

CURRENT IMPLEMENTATION CONTEXT

DoD's phased CMMC implementation has begun. Phase 1 runs from Nov. 10, 2025 through Nov. 9, 2026 and focuses primarily on CMMC Level 1 and Level 2 self-assessments. Contract language, data type, and solicitation requirements should drive your target level.

This checklist is built to help you turn a broad compliance requirement into a practical roadmap. Complete it once as a baseline, then revisit it monthly until you are ready for a formal assessment or affirmation.

HOW TO USE THIS GUIDE

1. **Classify your data.**
   Confirm whether you process, store, or transmit FCI, CUI, or both.
2. **Define your boundary.**
   Identify the systems, people, vendors, and locations connected to contract data.
3. **Score the gaps.**
   Prioritize missing controls, weak documentation, and unavailable evidence.
4. **Create the roadmap.**
   Translate findings into owners, timelines, and measurable milestones.

L1
FCI BASELINE

For environments that handle Federal Contract Information. Focuses on basic safeguarding requirements.

L2
CUI PROTECTION

For environments that handle Controlled Unclassified Information. Based on NIST SP 800-171 Rev. 2.

L3
ADVANCED PROGRAMS

For select high-priority programs requiring enhanced protection beyond Level 2.

BASELINE YOUR STATUS

CMMC readiness scorecard

02

Use this page as the executive summary for your CMMC program. Check completed items, add the point values, and use the score ranges at the bottom to determine your next step.

READINESS AREA	WHAT GOOD LOOKS LIKE	SCORE
1. Requirements confirmed	Contract clauses reviewed, FCI/CUI status documented, target CMMC level identified.	0 / 10
2. Assessment boundary defined	Systems, users, vendors, facilities, and data flows are mapped and reviewed.	0 / 15
3. Gap assessment completed	Controls, policies, tools, and operational processes have been assessed against the target level.	0 / 15
4. Remediation plan active	Gaps are prioritized by risk, assessment impact, owner, budget, and target date.	0 / 15
5. Documentation complete	SSP, policies, procedures, diagrams, inventory, and POA&M items are current.	0 / 15
6. Evidence available	Evidence is organized, current, repeatable, and mapped to assessment objectives.	0 / 20
7. Readiness review passed	Mock interviews, evidence review, and pre-assessment validation have been completed.	0 / 10

0-35

PLANNING STAGE

Start with contract review, data discovery, and boundary decisions.

36-60

ACTIVE REMEDIATION

Prioritize high-impact technical and documentation gaps.

61-80

PRE-ASSESSMENT

Focus on evidence maturity, interviews, and readiness validation.

81-100

ASSESSMENT-READY

Validate final evidence, scope, and operating consistency.

LEAD-GEN HOOK

Not sure how to score a section? Bring this workbook to a CMMC readiness consultation. Ironstack can help interpret your score and turn it into a prioritized roadmap.

1

Determine your requirements before buying tools.

03

Many organizations start remediation before they know what level applies. That can create unnecessary expense or leave critical obligations uncovered. Begin with a contract and data review.

CONTRACT REVIEW CHECKLIST

- ☐ Reviewed active and pending DoD contracts and solicitations.
- ☐ Identified clauses related to safeguarding, cyber incident reporting, NIST SP 800-171, and CMMC.
- ☐ Confirmed whether the work requires processing, storing, or transmitting FCI.
- ☐ Confirmed whether the work involves receiving, generating, or handling CUI.
- ☐ Validated subcontractor and flow-down obligations.
- ☐ Documented the target level and assessment type.

"The most expensive CMMC mistake is remediating the wrong scope."

DATA QUESTION	YOUR ANSWER
What FCI do we handle?	
What CUI do we handle?	
Where does it live?	
Who can access it?	
Who receives it?	

DECISION POINT

If you cannot clearly identify where FCI or CUI enters, lives, moves, and leaves your environment, pause remediation and perform discovery first.

2

Define the assessment boundary with intention.

04

Your boundary determines which systems, users, applications, locations, and external service providers must satisfy the target CMMC requirements. A smaller, well-designed boundary can reduce cost and assessment complexity without reducing security.

BOUNDARY WORKSHEET

- [ ] List every system that stores CUI.
- [ ] List every system that processes CUI.
- [ ] List every system that transmits CUI.
- [ ] Identify security protection assets that support the CUI environment.
- [ ] Identify contractor risk-managed assets and document rationale.
- [ ] Identify specialized assets and document handling assumptions.
- [ ] Map external service providers and cloud services.
- [ ] Review whether an enclave strategy would simplify compliance.

BOUNDARY RED FLAGS

Red flag: CUI is stored in general-purpose file shares with broad access.

Red flag: Email, chat, and collaboration systems are not classified by data type.

Red flag: Vendors can access CUI but responsibilities are not documented.

Red flag: Users copy CUI to unmanaged devices or personal cloud storage.

Red flag: Data flow diagrams are missing or outdated.

BOUNDARY ELEMENT	KNOWN TODAY	OWNER	NEXT ACTION
CUI systems			
Security tools			
External providers			
Facilities and users			

3

05

Assess controls, process maturity, and evidence readiness.

A gap assessment should not produce a generic deficiency list. It should produce a prioritized roadmap that accounts for business risk, assessment impact, operational effort, and evidence maturity.

GOVERNANCE

- Policies approved
- Procedures documented
- Risk process defined
- Roles assigned

ACCESS CONTROL

- MFA deployed
- Least privilege reviewed
- Privileged access controlled
- Access reviews tracked

ENDPOINT SECURITY

- Asset inventory current
- EDR/MDR active
- Encryption verified
- Patch process measured

LOGGING

- Logs centralized
- Retention defined
- Review cadence set
- Alerts triaged

INCIDENT RESPONSE

- Plan approved
- Roles documented
- Exercises completed
- Reporting path defined

VENDORS

- ESP list complete
- Cloud controls mapped
- Contracts reviewed
- Responsibilities assigned

ASSESSMENT READINESS LENS

For each requirement, ask three questions: Is it implemented? Is it documented? Can we produce recent evidence without scrambling?

4

Build a remediation plan that survives real operations.

06

Remediation should be prioritized by risk and assessment impact, not by whatever tool is easiest to buy. The goal is a roadmap that leadership can fund and teams can execute.

PRIORITIZATION CRITERIA

- Does the gap expose CUI or FCI to meaningful risk?
- Will the gap block a required assessment objective?
- Does the fix require policy, technology, training, or all three?
- Is evidence generated automatically after the fix?
- Who owns the control after implementation?

FIRST 30 DAYS

Confirm scope, close obvious high-risk gaps, assign owners, launch evidence repository, and finalize the remediation backlog.

DAYS 31-60

Implement core identity, endpoint, logging, vulnerability, and backup improvements. Draft required policies and procedures.

DAYS 61-90

Validate operating cadence, collect first evidence set, review SSP accuracy, and prepare for a readiness review.

BEYOND 90 DAYS

Mature evidence, test incident response, perform mock interviews, and resolve remaining documentation gaps.

GAP	RISK	OWNER	DUE DATE	EVIDENCE PRODUCED

5

07

Make documentation match reality.

Documentation is not paperwork for paperwork's sake. It is how you prove that your controls exist, your people know what to do, and your environment is managed consistently.

SSP CHECKLIST

- [ ] System description and business purpose documented.
- [ ] Assessment boundary and scope clearly described.
- [ ] Network and data flow diagrams included.
- [ ] Inventory of hardware, software, users, and services maintained.
- [ ] Control implementation narratives are accurate and testable.
- [ ] Roles and responsibilities are assigned to real people or teams.
- [ ] External service provider responsibilities are documented.

POLICY PACK

- [ ] Access Control
- [ ] Awareness and Training
- [ ] Audit and Accountability
- [ ] Configuration Management
- [ ] Incident Response
- [ ] Media Protection
- [ ] Risk Assessment
- [ ] System and Communications Protection

POA&M NOTE

POA&Ms are not a shortcut. CMMC Level 1 does not permit POA&Ms. Level 2 and Level 3 allow limited POA&M use under specific program requirements, and open items must be handled carefully.

DOCUMENT	STATUS	OWNER	LAST REVIEWED
System Security Plan			
POA&M			
Policies and procedures			
Diagrams and inventories			

6

08

Collect evidence before the assessment clock starts.

Assessments are evidence-driven. The best time to build your evidence process is months before an assessor asks for it. Evidence should be recent, repeatable, and tied to specific control objectives.

EVIDENCE TYPE	EXAMPLES	FREQUENCY	OWNER
Identity and access	MFA settings, access reviews, privileged account approvals, termination records.	Monthly / event-based	
Endpoint security	EDR status, encryption exports, patch reports, asset inventory.	Monthly	
Logging and monitoring	SIEM reports, alert triage tickets, log retention settings, review records.	Weekly / monthly	
Vulnerability management	Scan results, remediation tickets, exception approvals, retest evidence.	Monthly / quarterly	
Training	Security awareness records, role-based training, policy acknowledgements.	Annual / onboarding	
Incident response	IR plan, tabletop results, incident tickets, lessons learned.	Annual / event-based	
Change management	Change tickets, approvals, testing evidence, implementation records.	Event-based	

EVIDENCE QUALITY TEST

- Is the evidence dated?
- Does it identify the system or scope?
- Does it show the control operating?
- Can a non-admin retrieve it later?
- Is it mapped to a requirement or objective?

REPOSITORY STRUCTURE

Recommended folder structure: 01 Scope, 02 SSP, 03 Policies, 04 Evidence by Domain, 05 Vendors, 06 Training, 07 Incidents, 08 POA&M, 09 Readiness Review.

Tip: Name files with date, system, control family, and short description.

7

Run a readiness review before you schedule the assessment.

A readiness review is a dress rehearsal. It tests whether your documentation, evidence, control owners, and technical environment can withstand assessment-style review.

READINESS REVIEW CHECKLIST

- [ ] SSP reviewed for accuracy against the live environment.
- [ ] Assessment boundary reviewed by technical and business owners.
- [ ] Evidence sampled for completeness and currency.
- [ ] Control owners interviewed using assessment-style questions.
- [ ] Open findings assigned owners and due dates.
- [ ] Leadership briefed on residual risk and readiness score.

MOCK INTERVIEW PROMPTS

Access control: How do you approve, review, and remove access to CUI systems?

Incident response: Who leads the response, who reports, and where are records stored?

Logging: Which events are collected, how long are they retained, and who reviews them?

Configuration: How do you approve, test, and document system changes?

Vendors: Which providers support CUI systems and how are responsibilities defined?

FINDING	IMPACT	OWNER	FIX DATE	VALIDATED BY

WHEN TO ASK FOR HELP

If your team cannot explain scope, control implementation, and evidence collection in plain language, schedule a readiness consultation before pursuing a formal assessment.

TURN THE CHECKLIST INTO ACTION

Build your first 90-day CMMC sprint.

10

Use this page to convert your score into a practical execution plan. The goal is not to solve everything in 90 days. The goal is to create clarity, assign ownership, and build momentum.

PERIOD	PRIMARY OBJECTIVE	DELIVERABLES	EXECUTIVE DECISION NEEDED
Weeks 1-2	Confirm data and contract requirements.	Data inventory, target level, initial scope notes.	Approve target compliance path.
Weeks 3-4	Define the boundary and assessment approach.	Boundary diagram, system list, vendor list.	Approve enclave or enterprise scope.
Weeks 5-8	Perform gap assessment and prioritize fixes.	Gap register, risk ranking, budget estimate.	Fund remediation priorities.
Weeks 9-12	Start remediation and evidence collection.	Remediation backlog, evidence repository, draft SSP.	Approve readiness review timing.

EXECUTIVE OWNER CHECKLIST

- ☐ Named an accountable CMMC sponsor.
- ☐ Approved scope and budget assumptions.
- ☐ Committed department leaders to evidence responsibilities.
- ☐ Set monthly readiness review cadence.

DECISION LOG

DECISION 1

DECISION 2

DECISION 3

READY TO INTERPRET YOUR SCORE?

Use your completed checklist to start a focused CMMC conversation.

IF YOU SCORED 0-35

Start with data discovery, contract review, and boundary planning. Do not buy tools until scope is clear.

IF YOU SCORED 36-60

Move into active remediation. Prioritize controls that affect identity, endpoint security, logging, documentation, and evidence.

IF YOU SCORED 61-80

Focus on evidence maturity, SSP accuracy, mock interviews, and readiness validation.

IF YOU SCORED 81-100

Prepare final validation, confirm assessment expectations, and maintain evidence cadence.

Schedule a CMMC Readiness Consultation

Ironstack helps defense contractors assess readiness, define practical boundaries, prioritize remediation, and prepare the evidence needed for a smoother CMMC journey.

ironstacktechnology.com/cmmc

Bring this completed checklist to the call and ask for a roadmap based on your score, scope, and timeline.

OFFICIAL REFERENCES AND SOURCE NOTES

DoD CIO, CMMC Resources & Documentation: Phase 1 implementation timing and official program documentation. https://dodcio.defense.gov/CMMC/Resources-Documentation/

32 CFR Part 170, Cybersecurity Maturity Model Certification Program: program purpose, applicability, CMMC model, assessment requirements, and standards incorporated by reference. https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170

Federal Register, DFARS Case 2019-D041 final rule: contract implementation of CMMC requirements. https://www.federalregister.gov/documents/2025/09/10/2025-17359/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of

NIST SP 800-171 Rev. 2: protecting Controlled Unclassified Information in nonfederal systems and organizations. https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final

Planning disclaimer: This workbook is an educational readiness aid. It is not legal advice and is not a substitute for official contract review, assessor guidance, or applicable federal requirements.