CMMC Readiness and the Evidence Gap

A leadership guide for defense contractors

Use this guide to identify the evidence your team needs, decide what to investigate first and turn unresolved readiness questions into a company-wide plan.

A practical starting point

A leadership team needs more than confidence that security tools are installed. It needs a clear account of what applies to its business, what is working and who will address the remaining gaps.

The Smokejumper approach in this guide connects security work to the decisions that make it possible: scope, people, suppliers, funding, workflow changes and measures of completion. It is designed for defense contractors across manufacturing, services and technology.

Use the package	What you receive
Scope check	Six questions to establish what still needs clarification.
Evidence review	Fourteen questions across seven areas, with evidence prompts.
Execution review	Six questions about ownership, resources and follow-through.

These are planning diagnostics. They do not produce a CMMC status, a NIST assessment result or an SPRS score. A qualified review of all applicable requirements remains necessary.

Start with the requirement that applies

The current policy context

The July 13, 2026 announcement suspended the transition to CMMC Phase II and pending and future implementation milestones. It retained Phase I self-assessment requirements and the obligation to protect covered defense information. The current CIO guidance describes implementation as paused in Phase I. [S1, S2]

Start with the contract or subcontract, relevant amendments and the actual information flows. Have the contracts and security leads reconcile them with current official guidance. Do not build the business case around an obsolete November 2026 deadline.

Keep the standards and assessment route distinct

The current CIO guidance refers to NIST SP 800-171 Revision 2 for Level 2. NIST has separately superseded Revision 2 with Revision 3. A new publication does not by itself settle which revision your contract requires. Record the basis used for your review. [S2, S6]

Use the evidence review honestly

For each question, select Demonstrated, Partial, Absent or Unknown. Demonstrated means you can point to current evidence within the defined scope. Unknown means the respondent cannot yet establish the answer; it should never be silently converted into a compliant result.

Step	Decision
1 Clarify scope	Resolve the contract, information and system boundary.
2 Review evidence	Inspect the relevant records and operation of the process.
3 Build the plan	Assign owners, dependencies, resources and completion tests.

The seven areas on the following pages are a focused screening framework. They are not the complete set of 110 Level 2 security requirements. Treat a strong screening result as a reason to validate the broader position, never as permission to declare compliance. [S2]

Verify the foundation

1 Assessment and scope

A score has meaning only when the team can explain which systems, information and contract requirements it covers.

An outdated boundary can hide work, distort the budget and leave leaders relying on an unsupported statement of readiness.

Evidence to bring

Dated contract review, inventory and data flow map; system security plan owner. Assessment date, scope, evidence index and submission or affirmation records, as applicable.

The next management decision

Reconcile the contract register, system security plan and assessment record before making readiness representations.

Accountable roles: Contracts lead and security lead. Reference: S2 S3 3.12.1 and 3.12.4 S5.

2 Cloud and provider responsibilities

A provider claim does not establish what your specific service, configuration and customer responsibilities cover.

A cloud decision can create remediation work across email, backups, collaboration and the applications employees use every day.

Evidence to bring

Service and tenant inventory; applicable authorization or equivalency evidence; documented basis if no relevant cloud service is used. Responsibility matrix, service terms, evidence access and incident coordination arrangements.

The next management decision

Review each relevant service and tenant with its data types, security basis and division of responsibility.

Accountable roles: Security lead and procurement. Reference: S4 paragraph b 2 ii D.

Test how the organization responds

3 Incident response

An incident requires people to make decisions quickly while preserving information needed for investigation and reporting.

Unclear responsibilities can prolong disruption and leave contractual reporting steps unowned.

Evidence to bring

Approved response procedure, contacts, decision authority and reporting checklist. Dated exercise record, participants, lessons and tracked corrective actions.

The next management decision

Exercise a realistic incident with the people who would make containment, escalation and customer decisions.

Accountable roles: Security lead and executive sponsor. Reference: S3 3.6.1 to 3.6.3 S4 paragraphs c to g.

4 Configuration and changes

Changes to systems can alter access, introduce weaknesses or invalidate previous evidence.

Without a traceable change record, the team cannot reliably explain why a configuration differs from its agreed baseline.

Evidence to bring

Inventory, baseline settings, responsible owners and review dates. Change requests, impact reviews, approvals, test records and rollback arrangements.

The next management decision

Use a repeatable workflow for approving, testing, recording and reviewing relevant changes.

Accountable roles: IT operations and system owners. Reference: S3 3.4.1 to 3.4.5.

Connect detection to action

5 Monitoring and visibility

Leaders need to know which systems are visible, who reviews signals and how a concern becomes a response.

A tool can be deployed while coverage or follow-through remains incomplete.

Evidence to bring

Coverage inventory, monitoring configuration, review responsibilities and exceptions. Recent alert review records, escalation examples and documented dispositions.

The next management decision

Demonstrate coverage and escalation using a sample event from detection through disposition.

Accountable roles: Security operations and service providers. Reference: S3 3.12.3 3.14.6 3.14.7.

6 Vulnerabilities and remediation

Finding a weakness helps only when someone decides how and when it will be addressed.

Recurring findings and overdue actions can consume operating capacity and leave the same exposure unresolved.

Evidence to bring

Scan scope, schedule, recent results and the process for new vulnerability information. Finding register, risk decisions, owners, due dates and rescan or equivalent closure evidence.

The next management decision

Connect findings to owners, priorities, due dates and verification of the fix.

Accountable roles: Security lead and system owners. Reference: S3 3.11.2 3.11.3.

Control access and sequence the work

7 Access and least privilege

Access should follow a person or service account's actual responsibilities and be reviewed as those responsibilities change.

Unnecessary access increases exposure and makes accountability harder when staff, suppliers or systems change.

Evidence to bring: Role and access matrix, account approvals, privilege reviews and sampled configurations. Applicable multifactor authentication configuration; recent onboarding, transfer and removal records.

Next decision: Review privileged and ordinary access with business owners, including departures and role changes.

Accountable roles: IT identity lead and business managers. Reference: S3 3.1.1 3.1.2 3.1.5 3.5.3 3.9.2.

Plan around dependencies

For example, replacing a cloud service before confirming information flows can create avoidable migration work. Training employees before the target process is stable can require a second round of training. The sequence should follow the evidence and operating constraints.

Planning interval	Recommended output
First 10 business days	Confirm scope, review evidence and identify urgent weaknesses.
Next 20 business days	Assign priorities, resource estimates, dependencies and closure tests.
Following 60 days	Execute the agreed sequence, verify fixes and review remaining risks.

These intervals are a suggested management cadence, not a promise of compliance within 90 days. Actual timing depends on the starting position, system boundary, available staff and the work required.

Correct the assumptions that delay action

A paused phase means the security work can stop

Existing safeguarding obligations and applicable Phase I requirements remain. Verify the requirements for the specific work. [S1, S2]

A short questionnaire can certify readiness

This screening tool cannot establish all requirements or assess their implementation. It identifies questions for investigation and planning.

A cloud provider statement covers our whole environment

Check the exact service and the applicable authorization or equivalency basis, together with your responsibilities. Covered defense information in external cloud services has specific requirements. [S4]

Every gap can wait on a formal POA and M

CMMC permits only limited use of Plans of Action and Milestones. An internal improvement backlog is not proof that a gap qualifies for conditional status. [S2]

We need a particular ticketing product or a full time security desk to pass

The review should establish the required outcomes, evidence and responsibilities. Choose tools and staffing that support them; a product purchase does not establish compliance. [S3]

Bring the result into a leadership discussion

Complete the assessment with your contracts and security leads. Bring the three most important unresolved items, the evidence you already have and the business decisions that are blocking progress. Use that conversation to define a plan with owners, sequencing and measures.

Discuss your company plan with Smokejumper

Method and sources

What this guide is based on

This guide combines public primary sources with an original Smokejumper planning framework. It does not report survey findings or claim a measured prevalence of gaps among defense contractors. The scores in the companion tools describe a respondent's answers, not an independently verified security result.

The evidence checklist is selective. It does not cover every requirement in awareness and training, media protection, physical protection or other areas. Its category weights and result labels are editorial choices for planning and have not been statistically validated.

Policy context checked October 14, 2026. Recheck official guidance and the contract before using the package for a consequential representation or decision. The July 2026 suspension must be read alongside older rule and guide text.

S1 CMMC Phase II suspension announcement | July 13 2026

S2 CIO About CMMC and current assessment requirements | Accessed October 14 2026

S3 NIST SP 800 171 Revision 2 | February 2020 updated January 2021

S4 DFARS 252.204 7012 safeguarding and incident reporting | May 2024 clause accessed October 14 2026

S5 DFARS Subpart 204.75 | November 10 2025 text read with July 2026 suspension

S6 NIST Revision 2 publication status | Withdrawn May 14 2024 and superseded by Revision 3

CMMC means Cybersecurity Maturity Model Certification. CUI means Controlled Unclassified Information. SPRS means Supplier Performance Risk System. FedRAMP means Federal Risk and Authorization Management Program.