CMMC Supplier Readiness Roadmap

A Practical Guide for Primes and Suppliers

From flow-down requirement to an actionable readiness plan

When it comes to CMMC, a prime contractor's role is to determine what must flow down, communicate it clearly, and give suppliers a practical place to begin. The supplier is then accountable for its own readiness and implementation work.

HOW DO I KNOW WHICH CMMC LEVEL APPLIES TO MY SUPPLIER?

The required CMMC level depends on the information the supplier will handle and the requirements you flow down.

Federal Contract Information (FCI) generally requires **CMMC Level 1**.

Controlled Unclassified Information (CUI) generally requires **CMMC Level 2**.

Prime Contractor Guide

PRIME ACTION	PRACTICAL APPLICATION
1. Identify impacted suppliers	Determine which suppliers may handle FCI, CUI, or both.
2. Flow down the requirement	Include the clauses and cybersecurity requirements applicable to the subcontracted work and information.
3. Communicate expectations	Explain what applies, what information may be shared, and when readiness is needed.
4. Provide resources to get started	Provide a suggested starting point, such as the Supplier Starter Kit included in this guide. The supplier owns scoping, assessment, implementation, documentation, and assessment readiness.
5. Clarify prime-specific questions	Remain available for questions about the contract, data, and flow-down. When helpful, offer recommendations or introductions to qualified Managed Service Providers (MSPs), Cloud Service Providers (CSPs), Registered Practitioner Organizations (RPOs), and/or Certified Third-Party Assessment Organizations (C3PAOs).

Give Suppliers What They Need to Act

BE CLEAR ABOUT

- The applicable clause or safeguarding requirement
- Whether FCI, CUI, or both may be shared
- How information is expected to be exchanged
- The readiness date
- The point of contact for contract or data-flow questions

START WITH THE SUPPLIER STARTER KIT

Share the Supplier Starter Kit on the next page to help your supplier take the first steps.

→

Supplier Starter Kit

You received a cybersecurity flow-down. What should you do first?

Begin by understanding the contract and the information you will handle, then define the environment that needs to be protected either internally or with the support of a vendor.

YOUR FIRST 30 DAYS: BUILD CLARITY AND MOMENTUM

You do not need to solve everything at once. Focus on establishing a defensible baseline, identifying the highest-priority gaps, and creating a realistic action plan.

1 Understand the requirement	• Review the subcontract and applicable FAR/DFARS/CMMC flow-downs. • Confirm whether you will handle FCI, CUI, or both. Ask the prime to clarify the data and expected exchange when needed.
2 Define the scope	• Identify how the information will be received, created, accessed, processed, stored, transmitted, and destroyed. • Identify the people, devices, applications, cloud services, facilities, MSPs, and other parties that may touch the information.
3 Establish the baseline	• For an FCI/CMMC Level 1 path, evaluate the applicable basic safeguarding requirements. • For a CUI/CMMC Level 2 path, assess the applicable NIST SP 800-171 environment and establish baseline documentation such as an SSP, POA&M, and assessment score as applicable.
4 Decide how you will close gaps	• Prioritize gaps and determine what can be addressed through process, configuration, existing technology, or new technology. • Evaluate the full operating model, including users, MSP support, cloud/CSP choices, training, documentation, and ongoing cost.
5 Implement and sustain	• Implement the required protections and document how they actually operate. • Develop procedures, train users, maintain evidence, update documentation, and prepare for the assessment path that applies to your contract.

Questions to answer before selecting technology

- [ ] What information are we protecting: FCI, CUI, or both?
- [ ] Where will the information enter, live, move, and leave?
- [ ] What can our current IT/MSP support, and where do we need specialized assistance or CMMC advisory support?
- [ ] Who actually needs access?
- [ ] Can we limit scope with a separate environment or enclave?
- [ ] What will implementation and sustainment cost beyond year one?

THE #1 KEY TO CONTROLLING COSTS AND TIMELINES

Understand the requirements, define the scope, and establish a baseline before making technology and implementation decisions.

How Your Peers Are Putting Supplier Readiness into Practice

This real example shows how a prime can move from its own CMMC readiness to responsible supply-chain action—and how a supplier can respond in ways that protect both contract eligibility and its strategic partnerships.

Case Study: Convergint Federal + Chesapeake & Midlantic Marketing

PRIME: CONVERGINT FEDERAL | SUPPLIER: CHESAPEAKE & MIDLANTIC MARKETING

Convergint Federal is a prime contractor with CMMC Level 2 requirements. With support from Alluvionic's RPO team, Convergint Federal strengthened its program and achieved a **110/110** NIST SP 800-171 assessment score.

Chesapeake & Midlantic Marketing is a Convergint Federal supplier that provides physical security solutions.

SEE HOW THE PRIME AND SUPPLIER PUT IT INTO PRACTICE

Prime action	After strengthening its own program, Convergint Federal turned its attention to supplier readiness. It communicated the flow-down requirement, explained the readiness expectation, and introduced Chesapeake & Midlantic Marketing to an RPO.
Supplier starting point	Chesapeake & Midlantic Marketing confirmed what applied, identified the information and systems in scope, and established a practical readiness path.
Readiness work	With RPO support, Chesapeake & Midlantic Marketing completed a NIST SP 800-171 Basic Assessment, identified gaps, and developed its SSP and POA&M.
Implementation	Chesapeake & Midlantic Marketing addressed gaps, documented its environment, and submitted its SPRS score.
Outcome	Chesapeake & Midlantic Marketing maintained eligibility for DoD work, improved its security posture, and demonstrated responsible follow-through to its prime contractor.

WHAT GOOD EXECUTION LOOKS LIKE

Primes lead with clear requirements, early communication, realistic timelines, and useful connections—not by taking over the supplier's compliance work.

Suppliers protect contracts and key relationships by confirming scope, assessing gaps, documenting a plan, implementing improvements, and showing measurable progress.

ABOUT ALLUVIONIC

As an RPO and CMMC Level 2-certified organization, Alluvionic provides hands-on, solution-focused guidance and practical, right-sized support that has helped nine organizations achieve Level 2 certification.

Across more than 200 clients, this approach has earned 98% client satisfaction and helped defense contractors simplify CMMC, reduce internal burden, and protect contract opportunities.

Learn More: www.alluvionic.com