CMMC 2.0 is here. Are you ready?

The Department of Defense (DoD) holds information security as foundational to acquisitions and will independently verify mandatory DoD Cybersecurity regulations before contract award.

Malicious cyber activity targeting the Defense Industrial Base (DIB) undercuts US technical advantages and innovations in defense and significantly increases the risk to national security. The DoD created the Cybersecurity Maturity Model Certification (CMMC) as the cybersecurity standard for all DoD acquisitions to mitigate this risk. ***You are NOT ready if you do not know your CMMC maturity level***.

CMMC measures a company's ability to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI), combining various cybersecurity standards and mapping these best practices and processes to maturity levels, ranging from Foundational to Expert cyber hygiene practices. The CMMC effort builds upon existing regulations, specifically incorporating best practices from multiple sources. ***Significantly, CMMC adds an independent certification element to Advanced and Expert Levels to verify the implementation of cybersecurity requirements***; gone are the days of Cybersecurity self-certification. CMMC provides the DoD assurance that a DIB contractor can adequately protect CUI at a level commensurate to its risk, accounting for information to flow to subcontractors in a multi-tier supply chain.

Do you have the internal resources to become 100% compliant?

The Cybersecurity Maturity Model Certification (CMMC) framework consists of cybersecurity best practices and maturity processes from multiple Cybersecurity standards and frameworks, as well as inputs from the Defense Industrial Base (DIB) and Department of Defense (DoD). Thus, it provides a benchmark against which an organization can evaluate the current capability level of its processes, practices, and methods while setting goals and priorities for improvement. The CMMC compliance model contains 110 practices mapped across three maturity levels. Certification at Levels 2 and 3 will require a compliance assessment by an independent and sanctioned third-party assessor.

Defense Contractors must determine where they fall on the DoD's three-tier maturity level certification process and where they need to be to bid on DoD contracts. The intent is to identify the required CMMC level in RFP (sections L and M), and the maturity level be used as a "go / no go decision" by the Contracting Officer. The premise of CMMC is simple: The Department of Defense (DoD) will hold information security as foundational to acquisition — on par with cost, schedule, and performance — when awarding contracts. The new requirement builds upon existing Defense Federal Acquisition Regulation Supplement (DFARS) regulations by adding a verification factor to contractor cybersecurity controls and enhancing the protection of controlled unclassified information (CUI) within the supply chain. It is also critically important that Prime Contractors know where their Sub-Contractors fall on the DoD's three-tier maturity level certification process as they develop their DoD contract proposals.

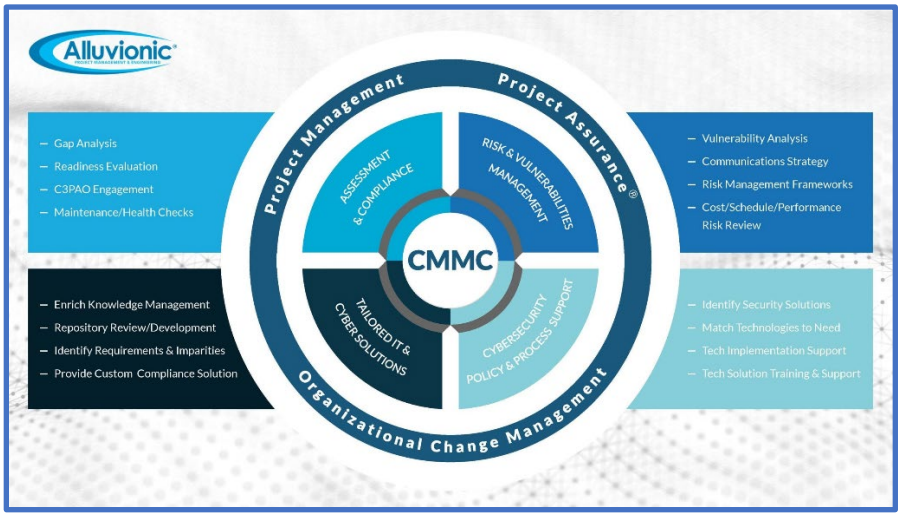
Defense Contractors recognize that cybersecurity is a business imperative, but few know how to implement it successfully. CMMC is not a one-time fix but a transformation towards more resilient cybersecurity.

Alluvionic® utilizes collaborative tools to develop a comprehensive picture of organizational cybersecurity resiliency. Your starting point is the same, whether assessing your cybersecurity posture for the first time or as part of your routine operations. The need for actionable information drives risk-based decisions and an effective management program to address any critical deficiency.

Alluvionic® can help you assess your cyber-resilience and build a comprehensive, strategic, and persistent risk management framework.

CMMC persistence is not a matter of organizational compliance, it is a matter of organizational change, and Alluvionic® is a leader in organizational change management. Techniques rooted in an understanding of organizational behavior facilitate communication, learning, and adoption of Cybersecurity changes. Utilizing a proven, disciplined process and team management, our CMMC advisors will:

- Provide a complimentary workshop outlining the objectives of CMMC and how we will reach your desired certification level.
- Analyze the current state of your cyber hygiene by applying our full-scope gap assessment scorecard.
- Develop remediation roadmaps for the most relevant risks to your program.
- Customize efficient and effective cybersecurity improvement plans.
- Provide risk granularity for your technical staff, comprehensive, actionable data for operational managers, and consistent strategic reporting to keep your C-Suite informed.
- Quickly mitigate your documentation gaps with pre-built policies & procedures, rapid change management application, and required service documentation.
- Cultivate growth toward a culture of cyber resilience.
- Instill confidence in your CMMC readiness at the board level.



3530 N Harbor City Blvd, Melbourne, FL 32925 USA Tel: +1 321 241 4510 www.alluvionic.com