Conquer Your Cybersecurity Certifications with Alluvionic®

A rapid change is occurring in the Defense Industrial Base (DIB) that impacts every company that aspires to do business with the federal government. It's called Cybersecurity Maturity Model Certification or CMMC. Whether you're a large, billion-dollar prime contractor or a single-scope small-budget subcontractor, CMMC will impact how you conduct business.

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 validating contractor cybersecurity controls to enhance the protection of controlled unclassified information (CUI) within the supply chain.

CMMC version 2.0, released on November 4, 2021, evolved the existing CMMC structure and introduced maturity levels ranging from "Foundational" (Level 1) to "Expert" (Level 3). DoD Contracting Offices will specify the required CMMC level in RFP sections L and M for use as a "go/no-go decision" in a contract award. An independent accreditation body manages the CMMC certification process that enforces the cybersecurity standard through audits, assessments, and training. Contractors can earn their CMMC certification through a certified, third-party assessment of their cybersecurity controls.

Two primary concerns for DIB contractors are:

- "How does my network measure up with the new standards?"
- "How does my compliance with NIST 800-171 (or other standards) fold into a CMMC certification?"

Unifying how people manage risk is a key component for an active, engaged, and integrated risk strategy.

Additionally, while leaders recognize that cybersecurity is imperative, they often have no implementation plans. Usually, companies either delegate the problem to IT, buy "the solution for everything" to spend their way out of it or treat it as a compliance issue. None of these approaches are effective if companies view cyber insecurity as a problem to be solved once rather than one that requires continuous mitigation.

Cyber risk is a risk management issue. Cybersecurity unifies your efforts to control cost, schedule, and performance. As a result, the cyber risk becomes a risk management issue, and the right questions become:

- "How much effort should we invest in keeping our company viable?"
- "Will our business operations continue when a system failure or adverse cyber event occurs?"

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

Alluvionic® employs collaborative tools such as *Cyber Secure Dashboard* from Heartland Science and Technology Group to develop a complete picture of organizational cybersecurity resiliency. Embedding risk management in the way people think and what they do day-to-day is vital for a robust and lasting implementation. Unifying how people manage risk is crucial for an active, engaged, and integrated risk strategy. Without it, a lack of commitment, incomplete data, and inconsistent tracking combine to cloud a firm's known risk exposure.

Alluvionic® can help you assess your cyber resilience and build a comprehensive, strategic, and persistent risk management framework. We will conduct an initial assessment of your cybersecurity posture and identify how cyber risk management can integrate into your daily operations. Regardless of where you are as a company, we can provide actionable information to drive risk-based decisions and effectively manage any 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 compliance; it's a matter of organizational change, and Alluvionic® is a leader in organizational change management. Techniques rooted in understanding organizational behavior facilitate communication, understanding, and adoption. Utilizing a proven, disciplined process in coordination with your team, 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 through the application of 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 tactical risk granularity for your technical staff, broad 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.

With all organizations facing a new regulatory reality of assessment for CMMC compliance by independent, sanctioned third-party assessors, Alluvionic® is ready to establish partnerships to meet these challenges and help reach any desired CMMC maturity goals. Alluvionic® provides Project Assurance™ by combining technical project management with organizational change and risk management to assure successful CMMC project delivery. By approaching each client's needs individually, Alluvionic® can customize solutions to the business' needs. With this personalized touch, we provide comprehensive solutions focused on managing risk — deploying risk management principles and philosophies from beginning to end.

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