CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

NEW CYBERSECURITY REQUIREMENTS COMING!

The new Cybersecurity Maturity Model Certification (CMMC) requirements established by the Department of Defense (DoD) will not be fully in place for all contractors and suppliers until 2026. However, your preparations should start now if you want to avoid losing out on lucrative government contracts. Be sure to complete the specific mandates under the DFARS Interim Rule to maintain contract eligibility until all audits can be completed.

Score Your Readiness

To start, you must be ready to conduct a self-assessment measuring your organization's cybersecurity posture for existing NIST 800-171 framework controls mandated with the DFARS interim Rule.

Upload Your Score

To retain eligibility for DoD contracts until CMMC certification is confirmed, you need to upload your score to the Supplier Performance Risk System (SPRS) portal right away.

Continuous Maintenance

Cybersecurity is a journey, not a single task or achievement. Start implementing the enhanced CMMC cybersecurity practices, which will go beyond the 110 existing security controls under NIST 800-171, expanding to include continuous threat monitoring and data protection.

Automation Tools

Take advantage of modern automation tools and analytics to further improve your organization's overall security posture and compliance with new CMMC framework standards.

Compliance Documentation

Having a structured process and specialized tools for the collection and organization of required records and current policies/ procedures will enable you to quickly and confidently present necessary evidence of compliance for audits or as part of attaining CMMC certification levels.

Compliance Will Intensify

When CMMC is fully rolled out, compliance will likely intensify. A qualified advisor can help your organization navigate CMMC complexities.

Start Your Journey toward CMMC Compliance.

Contact Us Today: info@utahip.org

UTAH INDUSTRY PARTNERS

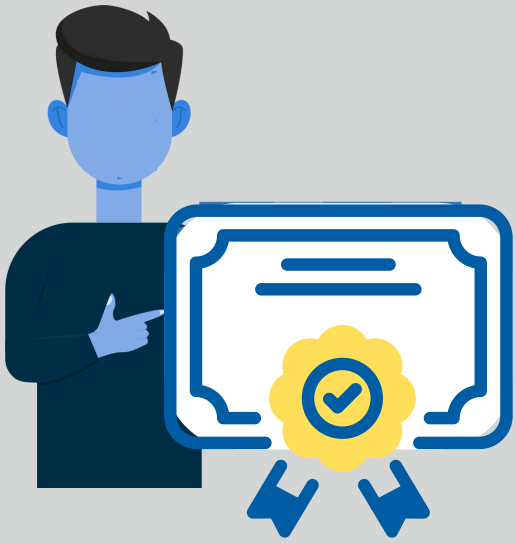
GEAR UP FOR CMMC COMPLIANCE

CMMC IS NOT ONE-SIZE-FITS-ALL

CMMC was designed to secure and improve the integrity of three types of data — Federal Contract Information (FCI), Controlled Unclassified Information (CUI) and Covered Defense Information (CDI) — stored on the information systems of federal contractors and their supply chain.

Depending on the type of data you process or store, the requirements of the DoD and your prime contractors, you will need to be prepared for CMMC certification level at one of its three levels. Once certified, you will be qualified to be awarded contracts at all levels up to your certification.

CMMC LEVELS 1, 2, & 3



CMMC Level 1 protects general contract information if you do not store or process CUI or CDI. Because the DoD contracts with many businesses for general supplies and services, it is estimated that 50% to 60% of defense contractors will just have to implement the 17 cybersecurity controls defined in CMMC Level 1.

If you do store or process CUI or CDI., you will need to be certified for CMMC Level 2's 110 cybersecurity controls made up of the 110 controls in NIST P 800-171. It is estimated that only a very small percentage of contractors will be required to be certified at Level 3.

Start Your Journey toward CMMC Compliance.

Contact Us Today: info@utahip.org