NEW CYBERSECURITY REQUIREMENTS COMING!

Is Your Business Ready?

Cybersecurity Maturity Model Certification

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.

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.

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

Detailed records and documentation are essential to effectively manage your compliance program requirements.

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

CONTACT US FOR MORE INFORMATION ABOUT HOW TO PREPARE YOUR BUSINESS FOR EXPANDED CYBERSECURITY MATURITY UNDER THE NEW CMMC FRAMEWORK.