mission multiplier

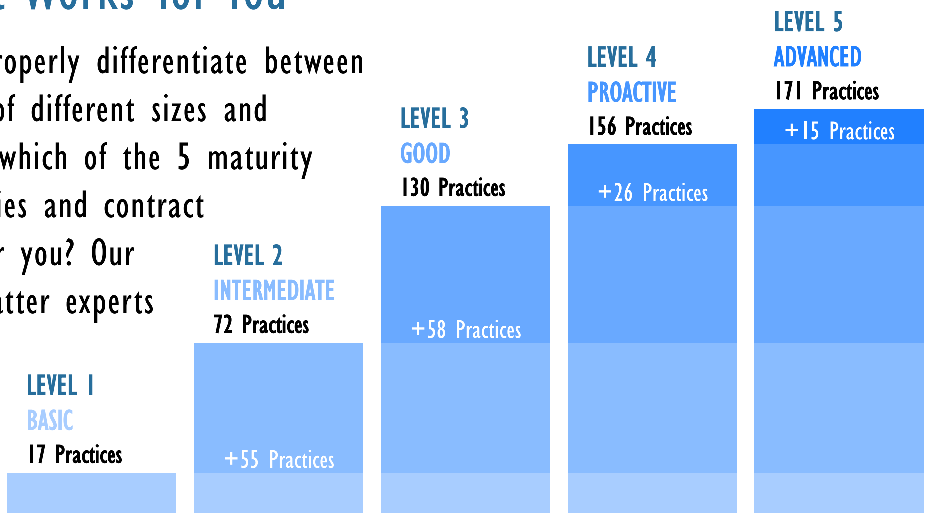
CMMC Compliance

The New Standard of Cybersecurity

The DoD's Cybersecurity Maturity Model Certification (CMMC) has breathed new life into the cybersecurity of the Defense Supply Chain. CMMC institutionalizes cybersecurity activities that are consistent, repeatable, and high-quality. It also introduces a requirement for contractors to have their implementation of these activities assessed by a third party before receiving certification. While this is a much-needed change for the integrity of the supply chain, it has left many contractors scrambling to fill gaps in their security and compliance processes that may have previously been unnecessary, unnoticed, or simply unaddressed.

Finding the Maturity Level That Works for You

Legacy compliance standards have failed to properly differentiate between the cybersecurity expectations for businesses of different sizes and capabilities. With CMMC, businesses determine which of the 5 maturity levels they need to pursue based on capabilities and contract requirements. Not sure which level is right for you? Our team can help. We have a team of subject matter experts that are well-versed in the requirements for each level, as well as the expectations for how the levels will correlate to various contract types.



Certification Just Got Serious

CMMC has done away with the self-attestation of compliance that contractors were able to take advantage of under previous standards. Gaming the system by producing a rudimentary SSP and perpetually POA&M-ing unimplemented controls is no longer an option. Failing to have all of the required cybersecurity practices and processes implemented and monitored before being assessed by a CMMC Third-Party Assessor Organization (C3PAO) could result in a failure to achieve the target level of certification and lead to a loss of contracts or inability to win new work.

Our team can conduct an initial review of your existing cybersecurity activities, then help you comply with the NIST SP 800-171 controls associated with your target maturity level, as well as the additional controls that CMMC has introduced. That way, when the time comes for your CMMC assessment, there won't be any unpleasant surprises.

mission multiplier

CMMC Compliance

Mission Multiplier’s Suggested CMMC Compliance Approach

CMMC compliance can be a challenge for small- to medium-sized companies. With the right approach, the implementation of the controls necessary for your target maturity level can go from being a costly source of stress and confusion to being a coordinated, streamlined process. Our approach focuses on separating controls into two easily understandable and manageable categories, capitalizing on existing assets, then filling the gaps with proven solutions.

The 2 Categories of Compliance Solutions: Services + Cyber Tools

Services

The Services category entails many of the services usually associated with an in-house Information System Security Officer (ISSO). These duties can be divided into the following domains:

- ✓ Policy
- ✓ Information Management
- ✓ Configuration
- ✓ Training

Cyber Tools

Tools are a natural part of any robust cybersecurity program. The tools required to satisfy most CMMC maturity levels primarily include:

- ✓ First Line Defenses
- ✓ Vulnerability Scanning/SIEM Solutions
- ✓ Malicious Code Protection
- ✓ Disk Encryption
- ✓ Multi-Factor Authentication
- ✓ Backup Infrastructure

Capitalize on Existing Assets

There is no need to replace assets that are already working. Mission Multiplier will assess your existing tools, systems, and people, show you how to utilize each to the fullest extent, then identify what you need to fill in the remaining gaps. If you have staff with some security and IT responsibilities, but not a dedicated ISSO, we can bolster your capabilities with our on-demand ISSO-as-a-Service offering. If you are missing important tools, we can recommend and help configure industry-leading, proven tools that will integrate seamlessly with your established infrastructure.

Get Ready for Certification

Once all areas have been addressed, it’s time to conduct a pre-assessment readiness review. Our team can guide you through, then help you make iterative improvements until you are fully prepared for your CMMC assessment.

HUBZone
Historically Underutilized Business Zone