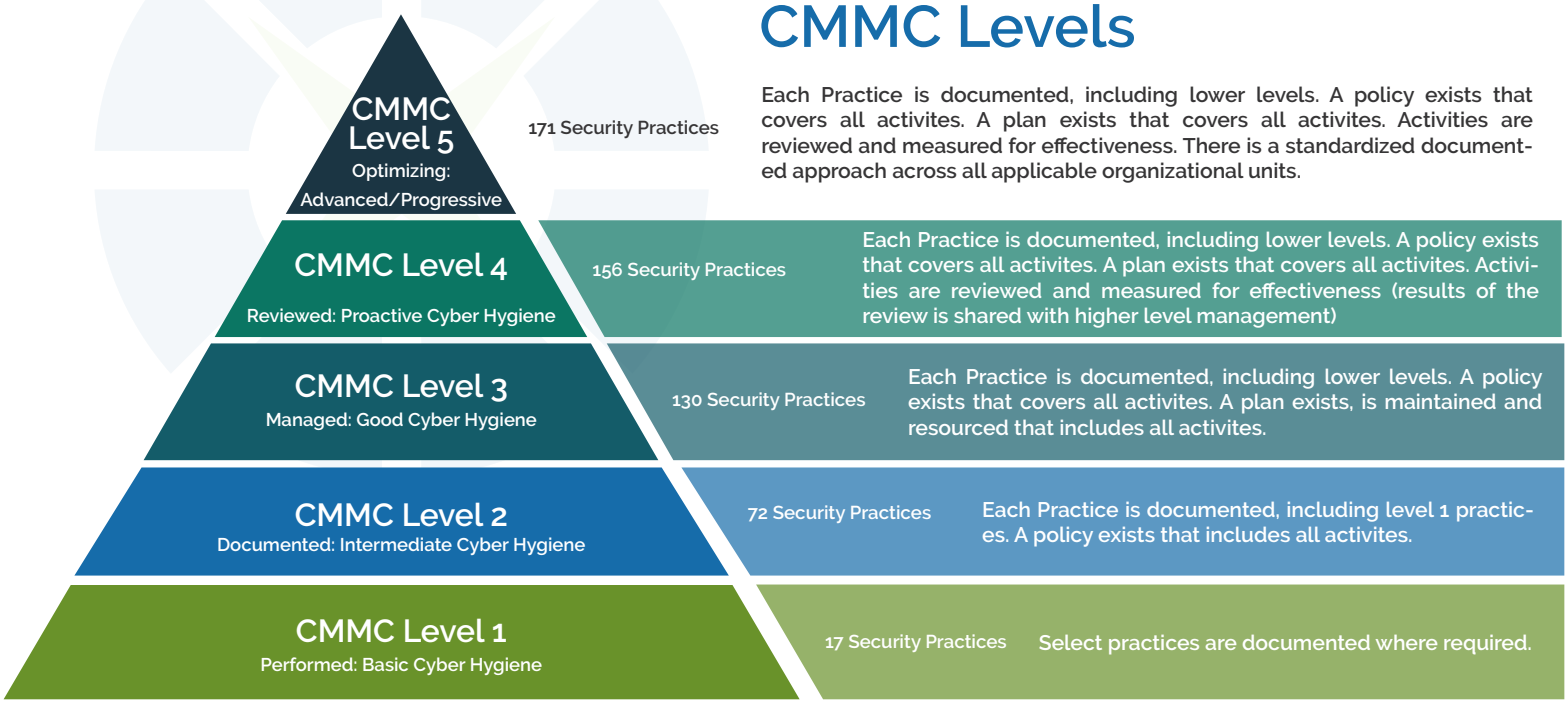
caetra.io™
Simplifying Compliance, Reducing Risk

CMMC Certification: What you need to know

The initial deadlines for the Cybersecurity Maturity Model Certification (CMMC) are approaching quickly and many U.S. Department of Defense (DoD) contractors are finding themselves unprepared to meet compliance. In previous years, DoD contractors were asked to self-certify their compliance with the NIST 800-171 Cybersecurity standards. However, in 2019 the DoD announced a new program known as the Cybersecurity Maturity Model Certification which will require contractors dealing with controlled unclassified information (CUI) to affirmatively prove their compliance with certain elements of NIST SP 800-171 through a third-party assessment.

CMMC Levels



CMMC Compliance is broken down into 5 Levels, each level building on the last. For example, Level One contains 17 cybersecurity controls, while Level 2 contains 72 (17 from Level one in addition to 55 additional practices). CMMC Controls are based on security controls from NIST 800-171, NIST 800-53, ISO 27001, ISO 27032, DFARS 252.204.-7012, and FedRAMP and together create the standards of compliance for DoD contractors/-subcontractors to follow regarding their internal systems and operations. Depending on the type of work you will be doing, or your subcontractors will be doing, you may want or need to aim for a specific CMMC Level. Read on to learn more about each CMMC compliance Level. Please note that CMMC has not yet been finalized and the controls and control composition of each level may change before the final version.

What CMMC level do I need?

A large plurality of contracts will likely require Level 3 compliance, and attaining these certifications can help your business obtain associated security certifications and DoD contracts.

CMMC Certification

Businesses looking to obtain a CMMC certification must pass an audit from a third-party assessment organization or credited individual assessor. CMMC does not allow businesses to self certify. The third-party assessment organization or credited individual assessor is known as the C3PAO.

C3PAO audit process

Before beginning the audit process, businesses seeking CMMC certification should identify the CMMC level they expect to be audited for and the desired maturity level they wish to attain. Next, a business must seek out an authorized C3PAO available to schedule the CMMC assessment with the independent assessor.

Proactive CMMC Certification

CMMC provides a set of clear guidelines for building an effective cybersecurity program that will not only stand up to regulatory scrutiny but can also reduce the risk of your organization suffering a significant data breach. Building a streamlined and coherent cybersecurity program is particularly critical for 2021 and beyond as the rate and complexity of cyberattacks continue to increase.

Do I pay for CMMC Certification?

The cost of a CMMC certification is considered an allowable, reimbursable cost by DoD and will be valid for three years after assessment.

What if I fail my assessment?

After the assessment, businesses will have up to 90 days to resolve any security issues found by the C3PAO and close any gaps necessary to obtain the desired results. If your company seeks an assessment for CMMC Level 3 and fails, you will not automatically obtain CMMC Level 2 certification. You will need to remediate any issues found in your audit and reassess within 90 days.