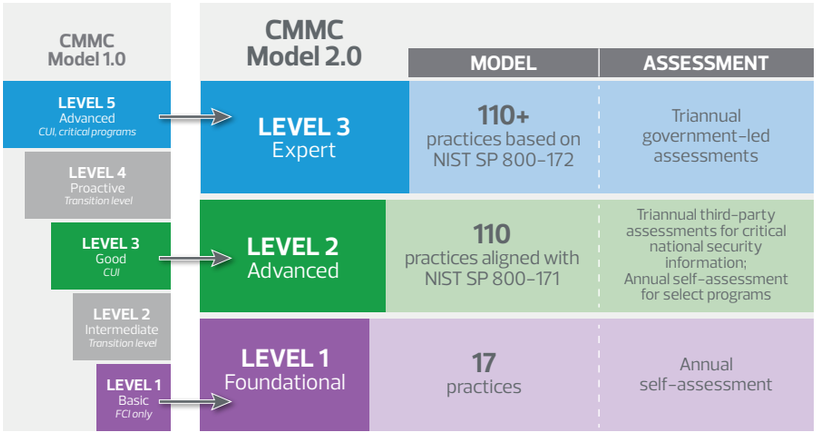
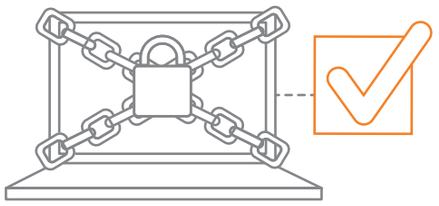
CMMC 2.0: 4 MAJOR CHANGES

1 Fewer cyber maturity levels



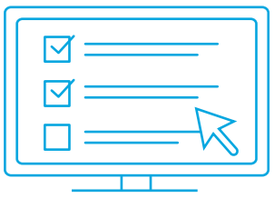
CMMC 2.0 has been restructured from five maturity levels to three levels of security. Levels 2 and 4 have been removed entirely to streamline the process.

2 Focus on NIST 800-171 and NIST 800-172



CMMC 2.0 will now place focus on the implementation of security requirements based on National Institute of Standards and Technology (NIST) Special Publication (SP) 800.171 and NIST SP 800.172, which in turn will reduce the number of security practices assessed.

3 Assessment requirements



Level 1 (foundational) will allow organizations to demonstrate compliance through self-assessments. The newly restructured **level 2** (advanced) will have bifurcated compliance expectations of both the self-assessment and independent certification requirements, based on the sensitivity of controlled unclassified information (CUI). And the new **level 3** (expert) assessments will be executed by the government on a triannual basis.

4 Allowance for POA&Ms

Under certain limited circumstances, CMMC 2.0 will now allow companies to make plans of action and milestones (POA&Ms) or allow waivers to achieve certification, despite maintaining known compliance gaps.

How does this affect my business?

If you work with the DOD, your organization is still required to design and implement a cybersecurity program aligned to NIST 800-171 during this transition period. Leveraging the industry experience of professionals like us at RSM is strongly encouraged to ensure eligibility to bid on future DOD contracts, which will soon require CMMC. Based on the DOD's estimate, it will take 9–24 months to fully implement CMMC 2.0 and for the mandatory requirement appear in all contract solicitations. Early adoption is strongly encouraged. For more details on CMMC 2.0, read our article.

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

ig-ar-nt-ras-bp-112a-cmmc regulatory update