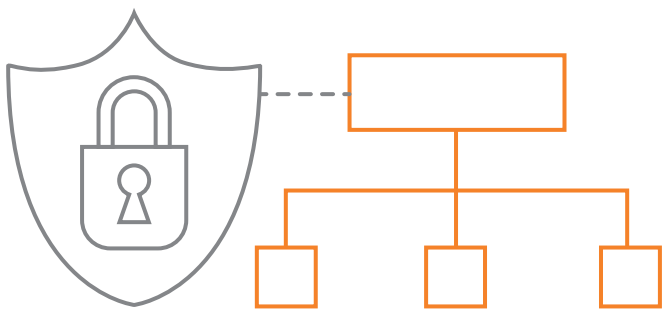
5 INDICATIONS you need Cybersecurity Maturity Model Certification advisory services

1 You provide goods and services to the Department of Defense (DoD)

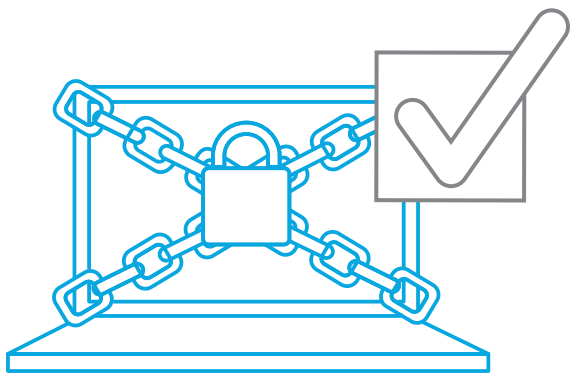
If your company has an active contract (or is pursuing one) with the DoD, you must become compliant and certified against CMMC security requirements.

2 You believe you are a subcontractor for an organization with a direct relationship with the DoD



If you are a subcontractor to a prime organization, whether your current DoD contract vehicle defines controlled unclassified information (CUI) or not, the underlying requirements for CMMC also flow down to your organization.

3 You believe that your organization already complies with DFARS 252.7012 and NIST 800.171

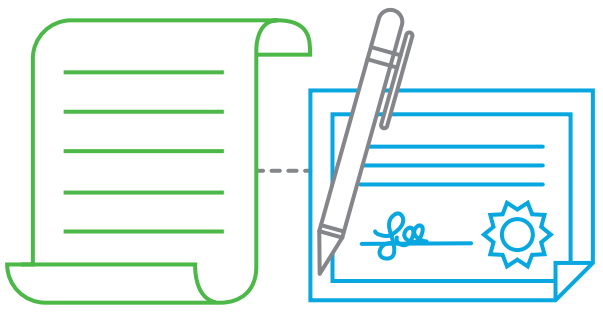


If you are compliant with those standards—that's great; that is the first major step for defining an effective cybersecurity program. NIST 800-171 was created as the self-assessment model. However, CMMC replaces NIST 800-171, and establishes the "trust but verify" expectation and adds new security controls that you must comply with.

4 You believe your current information security provider is an approved CMMC independent assessor

Unfortunately, as of March 2020, no organizations have yet been approved as third-party assessment organizations (C3PAO), as the accreditation body hasn't finalized the approval criteria. However, you can still conduct a readiness assessment to properly identify your CUI footprint and develop a sustainable cybersecurity program.

5 You don't know if CMMC applies to you



If you have an active DoD contract or you'd like to provide services to the DoD in the future, CMMC applies to you. Beginning June 30, 2020, and phasing in as contracts renew, RFIs and RFPs will require CMMC certification to a specified maturity level.

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

ig-nt-ras-all-0320-cmmc infographic

RSM