

CMMC Certification Preparation for DoD Contractors

CMMC – Cybersecurity Maturity Model Certification

Beginning in 2020, all contractors working for the DoD, even subcontractors must pass a CMMC Audit to ensure appropriate levels of cybersecurity controls and processes are adequate and in place to protect controlled unclassified information (CUI) on DoD contractor systems. We help DoD contractors prepare for their CMMC audit.

The CMMC Model

In its final form, the CMMC will intend to combine various cybersecurity control standards such as NIST SP 800-171 (Rev. 1 & Rev. B), NIST SP 800-53, ISO 27001, ISO 27032, AIA NAS9933 and others into one unified standard for cybersecurity. In addition to cybersecurity control standards, the CMMC will also measure the maturity of a company's institutionalization of cybersecurity practices and processes.



Pass Your Upcoming CMMC Audit with Confidence

ACT Security has helped DoD suppliers throughout the U.S. navigate the complexities of DFARS, NIST 800-171, and now CMMC.

We can help you...

- Do a Pre-Assessment for CMMC
- Develop an SSP and POA&M
- Implement the NIST 800-171
- Pass an upcoming CMMC audit

What We Currently Know About CMMC Certification and Audits

To verify that DoD Contractors have met the appropriate level of cybersecurity controls, the DoD will deploy certified independent 3rd party organizations to conduct audits on DoD Contractor information systems and inform risk. It is from this audit that a DoD contractor will be awarded a certification or not.

Important Dates and Milestones for DoD Contractors

Effective Immediately: Now is the time for contractors to get an assessment to determine where they stand regarding NIST 800-171 controls and the CMMC Level they want to achieve in order to be certified by the 2nd quarter of 2020.

4th Quarter of 2019: In Q4 of 2019, the DoD will release the CMMC Levels and their associated NIST 800-171A controls. The DoD will also announce the non-profit that will be in charge of the certification process and will start training 3rd party certifiers

January 2020: In January 2020 the official CMMC Levels and requirements will be released and the certifiers will be available soon thereafter to begin audits. There is likely to be a big backlog since there are approximately 70,000 companies requiring audits in a short timeframe and a limited supply of certifiers/auditors.

In June 2020 the CMMC requirements will be in Requests for Information (RFI's)

In late 2020 DoD contractors will need to be certified to bid on Requests for Proposal (RFP's).

Our expertise

<https://complianceandethics.org/read/nist-800-171-compliance-marathon/>
<https://complianceandethics.org/do-you-know-your-incident-reporting-compliance-responsibilities-under-nist-800-171/>

CMMC Audit Preparation & Assessment Services

ACTLLC has helped DoD contractors and their Primes throughout the U.S. navigate the complexities and financial hurdles of CMMC and NIST SP 800-171. We work closely with the DoD and are at the forefront of the latest cybersecurity frameworks that the DoD utilizes in CMMC. We have extensive knowledge and experience with implementing NIST and other frameworks' cybersecurity controls and can help DoD contractors prepare and successfully pass a CMMC audit and become certified.

TURNKEY SOLUTIONS

For more information on any of our products or services please visit us on the Web at: [HTTPS://www.actllc.io](https://www.actllc.io)

Prepare for a CMMC Audit

SERVICES AVAILABLE

- CMMC Gap Analysis
- POA&M Assistance
- SSP Assistance

Becoming Certified

DoD Contractors will need to coordinate directly with an accredited and independent third-party commercial certification organization to request and schedule a CMMC assessment. DoD Contractors will specify the level of the certification requested based on the DoD Contractor's specific business requirements. Contractors will be awarded certification at the appropriate CMMC level upon demonstrating the appropriate maturity in capabilities and organizational maturity to the satisfaction of the assessor and certifier.

Third party certification organizations will begin training in January 2020.

About CMMC Levels

The CMMC will review and combine various cybersecurity standards and best practices and map these controls and processes across several maturity levels that range from basic cyber hygiene to advanced.

Here's what we currently know about the CMMC levels and their respective requirements:

- Level 1** – "Basic Cyber Hygiene" – In order to pass an audit for this level, the DoD contractor will need to implement 17 controls of NIST 800-171 rev1.
- Level 2** – "Intermediate Cyber Hygiene" – In order to pass an audit for this level, the DoD contractor will need to implement another 46 controls of NIST 800-171 rev1.
- Level 3** – "Good Cyber Hygiene" – In order to pass an audit for this level, the DoD contractor will need to implement the final 47 controls of NIST 800-171 rev1. Plus, additional controls as required.
- Level 4** – "Proactive" – In order to pass an audit for this level, the DoD contractor will need to implement another 26 controls of NIST 800-171 RevB (still in the Public Comments stage)
- Level 5** – "Advanced / Progressive" – In order to pass an audit for this level, the DoD contractor will need to implement the final 4 controls in NIST 800-171 RevB.



340 Treeline Park Ste. 133
San Antonio, TX 78209
Phone 210.722.2479