Cybersecurity Maturity Model Certification 2.0 Checklist

Streamline your DoD Certification Process

Gather Information on CMMC 2.0

Before you get started, all primary stakeholders need to understand what the Cybersecurity Maturity Model Certification (CMMC) process is and the reasons Department of Defense (DoD) and Office of the Undersecretary of Defense – Acquisition & Sustainment (OUSD(A&S)) require it. CMMC increases security across the Defense Industrial Base (DIB) by unifying the measures DoD contractors take to safeguard sensitive information. CMMC 2.0 was released in late 2021, updating CMMC v1.02 to make implementation and assessment more uniform and accessible.

To learn more about the program, including how it has changed over the past few years, head over to the **CMMC website** and browse the **program overview** and **model breakdown**.

Select Your Assessment Level

Work with a qualified CMMC advisor or assessor to determine which Level of maturity your organization needs to reach, based on the contracts you're seeking with a DoD entity.

CMMC 2.0 comprises three Levels, in contrast with the five from CMMC v1.02:

Level 1: Foundational – Baseline protections for Federal Contract Information (FCI)

Level 2: Advanced – Protections for FCI and Controlled Unclassified Information (CUI)

Level 3: Expert – Proactive protections for advanced persistent threats (APT) to FCI/CUI

Note that Levels 2 and 3 correspond to Levels 3 and 5 from CMMC v1.02. If your organization had previously been required to attain those levels, you likely need their equivalents in 2.0.

Define the Scope and Cost

At this stage, you should connect with an RSI Security Account Manager or Sales Representative to estimate the total time, cost, and resources that will be required to complete certification. This includes both the implementation of controls to meet your desired level's requirements and any internal or external assessments required to verify certification.

To get started with estimating your scope, you can head over to the **CMMC Documentation** page and view the **Level 1** and **Level 2** scoping guidance documents. At Level 3 there at 134 unique Requirements for full certification, so please connect with an RSI Security Sales or Account Manager representative to begin scoping out an efficient compliance effort.

ABOUT RSI SECURITY

RSI Security is recognized by the CMMC-AB as an RPO, with technicians recognized as Registered Practitioners (RP). Our CMMC 2.0 services at present include readiness assessment and preparatory implementation to facilitate future certified assessments. With years of experience guiding contractors into NIST and DFARS compliance, we will prepare your organization for CMMC 2.0 and all future versions of the CMMC. Contact us to schedule a consultation and rethink your approach to CMMC implementation.

Cybersecurity Maturity Model Certification 2.0 Checklist

Streamline your DoD Certification Process

Implement Framework Controls

Here is where the most intensive work begins. Your RSI Security Assessor and Project Manager can assist with shaping your current People/Process/Technology environment to meet the exact specifications of your desired CMMC Level.

CMMC 2.0 certification requires implementing an increasing amount of the National Institute of Standards and Technology's (NIST) **Special Publications 800-171** and **800-172** at each level:

Level 1 – 15 Requirements sourced from NIST SP 800-171. These are primarily "Basic" Requirements in SP 800-171, lining up with the Level 1 "Fundamental" designation.

Level 2 – 110 Requirements, comprising all of SP 800-171. These are both "Basic" and "Derived" Requirements, corresponding to the Level 2 designation of "Advanced."

Level 3 – 134 Requirements, including all of SP 800-171 and 24 from SP 800-172. These are referred to as "Enhanced" Requirements, mirroring Level 3's "Expert" designation.

Refer to the NIST documents linked above for a full breakdown of the Requirement Families and Requirements—Basic, Derived, and Enhanced—you need to implement for Level 1, 2, and 3.

Conduct Self or Third-Party Assessment

Get a professional CMMC assessor from RSI Security to review your implementation.

Organizations at Level 1 and some at Level 2 may be able to self-assess annually. See the **Level 1 Self-Assessment Guide** and **Level 2 Self-Assessment Guide** for more information on these. Most organizations at Level 2 will need triennial third-party assessments conducted by assessors vetted by the Cyber AB vets. All organizations at Level 3 require triennial, government-led assessments to maintain certification.

Regardless of Level, however, third-party preparatory assessments are critical to success.

Maintain Your Certification Long-Term

Certification with the DoD is not permanent; all organizations will need to regularly re-assess their implementation at different intervals depending on Level (see above). And, if anything about your organization's security changes between these assessments, or you begin to process new kinds of information that would require a higher Level of maturity, you'll need to consider implementation a longer-term process, as well.

Hence the importance of a compliance partner like RSI Security.

Working with a CMMC implementation partner like RSI Security will streamline the process of achieving and then maintaining your DoD contractor status long-term. We'll help to shape and update controls,