Deltek

Understanding Cybersecurity Maturity Model Certification (CMMC) 2.0 Compliance

A Government Contractor's Guide to Preparation and Assessment Basics

The History of CMMC

The Cybersecurity Maturity Model Certification (CMMC) was created to safeguard sensitive unclassified information across the Defense Industrial Base (DIB) by addressing the gaps in prior regulatory requirements. The Department of Defense (DoD) found that private sector organizations doing business with the federal government were not satisfying the requirements specified in Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012. The requirements included implementation of National Institute of Standards and Technology (NIST) SP 800-171 for systems processing Covered Defense Information, but did not include official certification or compliance reporting mechanisms. This resulted in organizations not fully implementing controls to a consistent maturity level, ultimately putting the government supply chain at risk. Since an official certification or compliance reporting mechanism did not exist, many companies fell short of their security control obligations, putting the government supply chain at risk.

Once final, the CMMC certification requirement will be enforced by the presence of the DFARS 252.204-7021 clause, which will specify the CMMC Level (1-3), whether an external audit is required and other relevant details to ensure consistency across the DIB.

The Final CMMC Program Rule (32 CFR Part 170) was published in the Federal Register on October 15, 2024 and the CMMC Phased Rollout is expected to begin mid-2025.

CMMC addresses requirements for the protection of FCI and CUI data:

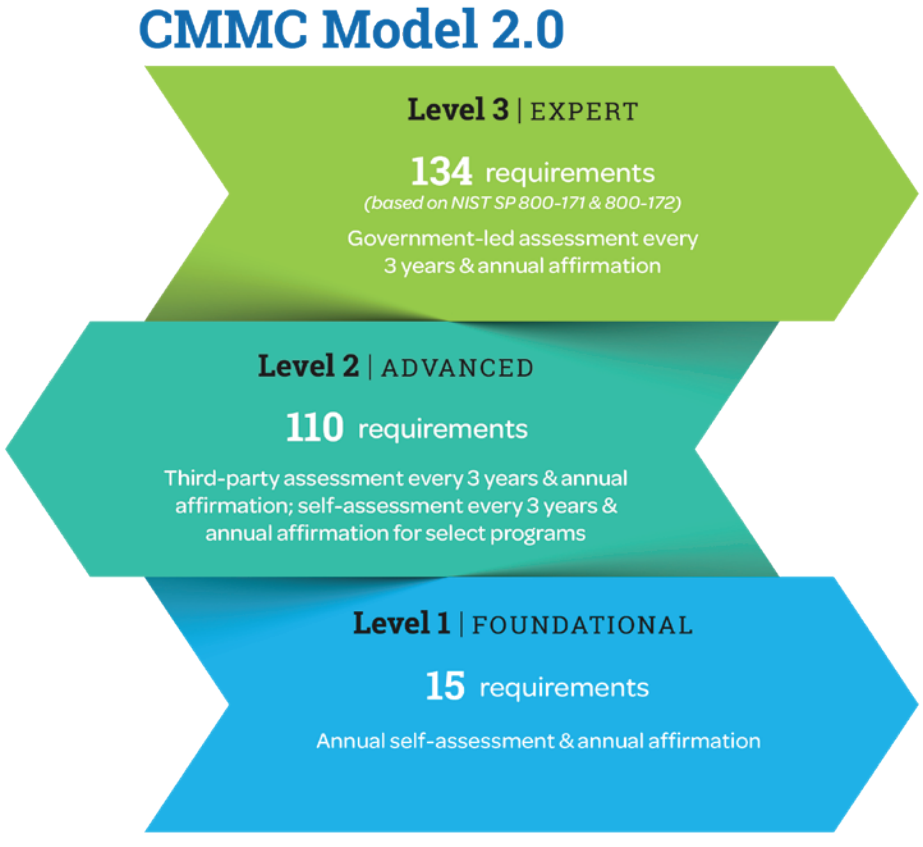
- **Federal Contract Information (FCI)** - Information not intended for public release. It is provided by or generated for the government under a contract to develop or deliver a product or service to the government. FCI does not include information provided by the government to the public.
- **Controlled Unclassified Information (CUI)** - Information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

As stated by Acquisition & Sustainment, Office Under the Secretary of Defense, CMMC 2.0 requires that companies entrusted with national security information implement cybersecurity standards at progressively advanced levels, depending on the type and sensitivity of the information. The program also sets forward the process for information flow down to subcontractors.

Three CMMC Certification Levels

CMMC 2.0 streamlines the model to three compliance levels:

- **Level 1** – Foundational, which allows organizations to conduct self-assessments, against FAR 52.204-21.
- **Level 2** – Advanced, includes 110 practices from NIST SP 800-171 and allows for self-assessment for some Controlled Unclassified Information (CUI), but requires Certified Third Party Assessment Organization (C3PAO) to conduct assessments when working with sensitive, prioritized CUI.
- **Level 3** – Expert, requires CMMC 2.0 L2 C3PAO certification, adds a subset NIST SP 800-172 controls, and requires an assessment from the DoD when working with the most sensitive controlled information.



**The New CMMC 2.0 Levels Map Directly to NIST 800-171 Controls.*

The CMMC Level certification requirements will be driven by the type of data being stored/processed/handled to support a contract with the DoD. In general, FCI and basic CUI such as government-provided PII and financial data will require a Level 1 certification. More sensitive covered defense information (CI) such as purchase orders, parts lists, and inventory may require a Level 2 certification, and technical documentation such as blueprints for military aircraft, could require a Level 3 certification. Contracts will specify the CMMC Level required to be eligible for the DoD contract.

The DoD has adjusted and streamlined the CMMC accreditation program with CMMC 2.0.

This new version will be focusing on the most advanced cybersecurity standards while minimizing barriers to compliance. This new approach will require additional accountability for organizations to implement critical cybersecurity standards to meet the challenges of evolving threats and take the necessary steps to protect national security information.

Key CMMC Players

Assessors: Individuals who have successfully completed the background, training, and examination requirements as outlined by the CMMC Accreditation Body (AB), and to whom a license has been issued. Assessors are not employed by the CMMC-AB and may or may not be employed by the Certified Third Party Assessment Organization (C3PAO).

Certified Third Party Assessment Organization (C3PAO): Design after the colon, replace the description with: An organization that has been authorized or accredited by the Accreditation Body to conduct Level 2 certification assessments.

CMMC Accreditation Body (AB): The accreditation body that establishes and oversees a qualified, trained, and high-fidelity community of assessors that can deliver consistent and informative assessments to participating organizations against a defined set of controls/ best practices within the CMMC program.

Organizations Seeking Assessment (OSA): The organization that is going through the CMMC assessment process to receive a level of certification for a given environment.

Organizations Seeking Certification (OSC): Entity seeking to undergo a certification assessment for a given information system for the purposes of achieving and maintaining the CMMC Status of Level 2 or Level 3.

Cloud Service Providers (CSP): An external company that provides cloud services based on cloud computing (defined in NIST SP 800-145) that stores, processes or handles CUI on behalf of an OSA. CSPs must be FedRAMP Authorized at the Moderate (or higher) baseline; OR meet the equivalent security requirements in accordance with DoD Policy.

External Service Provider (ESP): The external people, technology or facilities that an organization utilizes for provision and management of IT and/or cybersecurity services on behalf of the organization. In the CMMC Program, CUI or Security Protection Data, must be processed, stored or transmitted on the ESP assets to be considered an ESP.

Day-to-Day Impact for Government Contractors

Most organizations fulfilling government contracts for the DoD will need to address CMMC requirements in requests for information (RFIs) and requests for proposal (RFPs) bids for DoD acquisitions, with the potential exception for commercial items.

The various cybersecurity standards and best practices upon which the CMMC is based are largely self-certified. The CMMC represents a major change to that by introducing the C3PAO requirement to review systems and processes for certification. To standardize this process, the DoD established the non-profit, independent organization, CMMC-AB, to define the assessment and administration needed for certification. Currently, the CMMC-AB is in the process of licensing assessors and the firms that will serve as C3PAOs.

Government contractors will initially see DoD requirements to satisfy Levels 1 and 2 for anyone handling FCI or CUI. The majority of contractors will need to certify first at Level 1 and then Level 2. Level 3 will be required for organizations working with the most sensitive CUI or confidential data, however, it will be required to first certify at Level 1 and Level 2 before Level 3. Level requirements will be specified in contracts and are expected to flow down only to subs that are working with the controlled information. Therefore, it is important to know what type of data you are storing. Once an organization is CMMC certified, the certification is expected to be valid for three years, with the potential for an annual attestation requirement depending on the level certification requirements."

Preparing for CMMC 2.0

To ready their organizations, government contractors should ensure they cover the following steps.

- **Step 1** – Identify and classify the type of data you store to support existing or new contract awards.
- **Step 2** – Understand the Level your firm will likely need to satisfy based on the type of data you store and identify the gaps that could prevent achieving certification.
- **Step 3** – If you are unsure and work with CUI, start with Level 2, based off the 110 controls from NIST 800-171.
- **Step 4** – Make sure you have the documentation of formalized processes and controls.
- **Step 5** – Be familiar with all of the major definitions and compliance standards that make up CMMC 2.0. In addition, be sure any External Service Providers have the required security certifications and can provide a customer responsibility matrix (CRM).

Leveraging cloud service providers can be a solid strategy for addressing many aspects of CMMC 2.0. For instance, the controls implemented in Costpoint GovCon Cloud Moderate support DFARS 252.204-7012 and NIST SP 800-171 requirements which, were adapted to form the basis of the CMMC framework. However, simply moving into the cloud does not automatically make a firm compliant. But, it can assist with getting to certification quicker and with less cost.

Key considerations when looking at a vendor for a cloud solution:

- Is the cloud solution designed for use in the government contracting space and does the provider understand the necessary security requirements?
- Can the Cloud Service Provider (CSP) demonstrate the required security needed for your CMMC certification (FedRAMP Moderate equivalence)?
- IMPORTANT: Verify your CSP's compliance with the FedRAMP Moderate baseline controls if they are not listed on the FedRAMP Marketplace. This is a requirement for CMMC Level 2 & 3 certification.
- Any Cloud Service Provider (CSP) storing, processing or transmitting Controlled Unclassified Information (CUI) needs to also conform with DFARS clause 252.204-7012, which includes additional requirements.
- Trust, but verify. Request the Customer Responsibility Matrix (CRM) and confirm that your CSP meets the required standards for your CMMC certification BEFORE you waste your precious time and money with a provider that cannot meet the standard.

Readiness Checklist

An additional step to ensuring CMMC 2.0 compliance is to take a closer look at networks and procedures within your business. Conducting a third-party readiness assessment will determine whether your organization is prepared to meet the appropriate Level in terms of system setups and processes, or where it is inadequate or does not completely meet the defined requirements.

What will be scrutinized during the gap analysis?

- Where data is stored or processed
- Training of information managers and administrators
- Access to systems includes several security controls and an IRP is a required control
- Access to information systems
- Development and implementation of incident response plans
- Supplier and subcontractor relationships and their role in the supply chain

Those seeking CMMC 2.0 compliance will need to go through the added step of proving their ability to report on how they will detect, alert and respond to system and data threats.

Remediation Planning

A remediation plan will begin to emerge from the findings of the readiness assessment. It will likely involve a change to people, process, or technology to ensure they meet the cybersecurity standards as outlined in CMMC 2.0. The assessment should identify areas that require prioritization, help define completion timelines, estimate costs and aid with goal and milestone tracking to reach the required Level. Documentation will play a big part in executing on a remediation plan.

How Deltek Can Help Government Contractors Get Ready for CMMC 2.0

It's no secret that cybersecurity compliance regulations continue to evolve and become more prescriptive. With the increased activities of hackers and cybercriminals, it's critical to your business operations to stay ahead of regulations like CMMC 2.0 – and be prepared.

Deltek is dedicated to protecting your data by ensuring our capabilities meet the constantly changing security landscape. We are continuously adjusting our suite of products and services to support your cyber posture by increasing its investment in security, compliance and supporting technologies for our customers – easing and scaling the management of systems for your teams.

The DoD has mandated that all government contractors competing for DoD contracts are CMMC 2.0 certified. While this mandate may seem to be in the distant future, many government contractors are planning ahead, making it a top priority to find a CSP that offers a solution that will support their CMMC 2.0 compliance requirements. It's important to invest in a CSP and a solution that helps address all of your requirements as a one-stop-shop, partnering with you as new compliance initiatives develop in the future, with the understanding that compliance frameworks are a shared responsibility.

We continue to evolve and refine our strategies as a committed business partner to help customers safeguard their protected data by designing and operating services that align with multiple compliance frameworks. Our existing Costpoint GovCon Cloud solutions have:

- Fully implemented NIST 800-171 controls
- Implemented FedRAMP Moderate controls with the Costpoint GovCon Cloud Moderate environment
- Incorporated CMMC 2.0 framework into our cloud compliance and security posture

Deltek's Costpoint GovCon Cloud provides benefits beyond what a traditional on-premise or hosted solution can provide. Through the power of Deltek's Cloud, businesses of all sizes can easily prepare for the ever-changing compliance requirements, like those presented in CMMC 2.0, while confidently and securely maintaining data within a secure cloud environment that is continuously refined to meet the most up-to-date government and agency cybersecurity compliance standards.

Also, Deltek helps the industry stay informed on some of these topics like CMMC 2.0 and other cybersecurity trends. The GovWin IQ Federal Opportunities product allows users to search for opportunities that contain CMMC 2.0 requirements, as well as the specific certification level required for contractors that are bidding on that opportunity. GovWin IQ provides more insight and visibility into those opportunities that will have very specific requirements around CMMC 2.0. As part of the GovWin IQ market analysis and information services solution, new content and resources are constantly released and refreshed, providing key analysis of DoD initiatives, plus insight into how companies are responding (or should be responding).

What Our Customers Are Saying

LMI, a consultancy dedicated to powering a future-ready, high-performing government by drawing from expertise in digital and analytic solutions, logistics, and management advisory services has already made the decision to move to Costpoint's GovCon Cloud Moderate solution. "LMI decided to move to the Deltek Cloud to support our digital transformation strategy necessary to grow our business without investing in additional operations staff," said Jim McNabb, Senior Project Manager at LMI. "Additionally, 60% of our business comes from DoD work so we wanted to get ahead of CMMC requirements. Deltek's Costpoint GovCon Cloud Moderate solution will provide us with peace of mind on our financial system so the rest of our organization can focus on more strategic tasks."

FedRAMP

What's on the Horizon for Deltek? What's Next for Your Business?

Deltek Costpoint GCCM has achieved FedRAMP Moderate Ready status and is listed on the FedRAMP Marketplace to support cybersecurity compliance requirements for government contractors.. We are also diligently watching for any updates or changes to the certification process from DoD that could potentially impact our customers. Now that the details of the CMMC program have been released, it is time to partner with the leading purpose-built ERP for GovCons that will support your CMMC compliance initiatives.

It's important to remember that compliance frameworks are a shared responsibility between the CSP and the user. Therefore, it's imperative for your business operations to know what is required to meet and maintain compliance, as well as remain eligible for specific types of contracts. Our cybersecurity compliance experts are keeping up with industry requirements as they evolve, so rest assured the Costpoint GovCon Cloud environments are a secure arena that enable you and your teams to continue doing business as usual within Costpoint with the necessary support to maintain compliance with federal requirements.

Deltek

Browse more content at **deltek.com/resources »**

Better software means better projects. Deltek is the leading global provider of enterprise software and information solutions for project-based businesses. More than 30,000 organizations and millions of users in over 80 countries around the world rely on Deltek for superior levels of project intelligence, management and collaboration. Our industry-focused expertise powers project success by helping firms achieve performance that maximizes productivity and revenue. **deltek.com**