INTELLIGENT TECHNICAL SOLUTIONS

EVERYTHING YOU NEED TO KNOW ABOUT CMMC 2.0 IN 2023

A Quick Guide to the Updated Cybersecurity Maturity Model Certification

TABLE OF CONTENTS

INTELLIGENT TECHNICAL SOLUTIONS

INTRODUCTION

If you're a compliance officer, a DoD contractor, or part of the DIB sphere, you're probably aware of the Cybersecurity Maturity Model Certification. But what exactly is it? And how does this new standard change the way companies are required to manage and implement their compliance programs?

This eBook explores these questions and gives insight into what you need to know if your company is thinking about going through this process.

WHAT IS CMMC 2.0?

The Cybersecurity Maturity Model Certification (CMMC) 2.0 is the simplified version of the CMMC framework, which was created by the U.S. Department of Defense (DoD) to improve the cybersecurity posture of the Defense Industrial Base (DIB) and its supply chain.

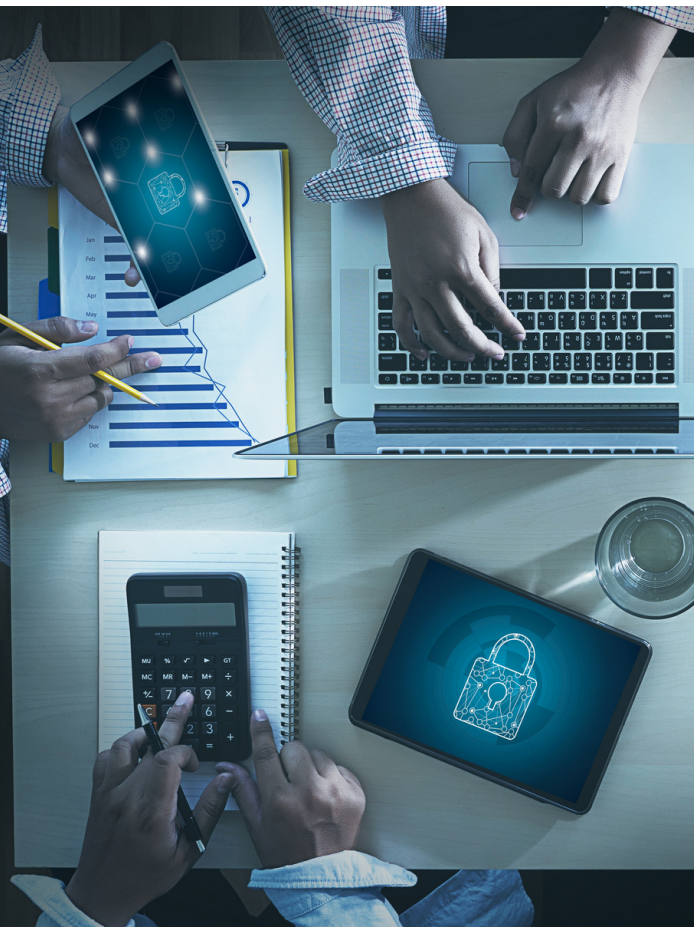
CMMC 2.0 is a tool for assessing the cybersecurity maturity of an organization. It brings standardized cybersecurity into the DIB, providing a common language and framework for all participants in this space.

It is the culmination of several years of work by government and industry stakeholders who recognized the need to develop a voluntary framework to help assess cybersecurity maturity levels and improve national security. **Organizations aiming for CMMC certification must adapt to the updated guidelines by May 2023.**

The CMMC 2.0 framework includes three levels of increasing maturity, ranging from Level 1 (basic cyber hygiene) to Level 3 (advanced/progressive). Each level has specific requirements that organizations must meet to achieve certification.

INTELLIGENT TECHNICAL SOLUTIONS

HISTORY OF CMMC



CMMC, despite being formalized in 2019, has its roots in the 2002 Federal Information Security Management Act, which required each federal agency in the United States to provide information security for the information and information systems.

Eventually, through the efforts of the NIST (National Institute of Standards and Technology), further standardized guidelines for cybersecurity emerged. In 2019, the Department of Defense finalized the CMMC as a tool to evaluate if government contractors and suppliers followed the basics of NIST's Cybersecurity Framework.

During the implementation of CMMC, the DoD noted the concerns of those affected by the new standards. They then further simplified the approval processes and implementation guidelines, which resulted in the CMMC 2.0 today.

WHAT IS THE GOAL OF CMMC 2.0?

The goal of CMMC is to provide organizations with a common language and set of metrics that will enable them to better understand their current state of cyber-readiness and prioritize future improvements.

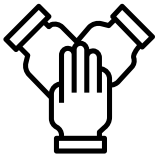
INTELLIGENT TECHNICAL SOLUTIONS

BENEFITS OF CMMC 2.0

CMMC 2.0 is the latest version of this CMMC, and it includes several new features and updates intended to improve its effectiveness.
Some of the benefits of CMMC 2.0 include the following:

Improved security
CMMC 2.0 includes updated requirements and best practices for protecting sensitive information, which can help organizations better defend against cyber threats.

Increased accountability
CMMC 2.0 includes new certification levels and a third-party certification process, which can help ensure that organizations meet the necessary security standards.



Enhanced collaboration
CMMC 2.0 includes new provisions for information sharing and collaboration among organizations in the defense industrial base, which can help to improve information security across the DIB.

Greater flexibility
CMMC 2.0 includes a new tiered structure that allows organizations to choose the level of certification that is appropriate for their needs, which can help to reduce the burden of compliance for smaller organizations.

Overall, CMMC 2.0 is designed to provide a more comprehensive, practical, and flexible approach to protecting sensitive information from cyber threats in the defense industrial base.

INTELLIGENT TECHNICAL SOLUTIONS

CMMC 1.0 VS. 2.0

The most significant change between CMMC 1.0 and 2.0 is that there are now three levels of accreditation instead of five (and no quick start option). The purpose of this change was to simplify certification processes by grouping similar competencies into fewer categories.

WHAT ARE THE LEVELS?

Instead of five levels of certification, CMMC 2.0 simplified it into only three levels: Foundational, Advanced, and Expert.

Source: National Institute of Standards and Technology (NIST)

LEVEL 1

FOUNDATIONAL

The first level is for companies handling Federal Contact Information (FCI). It requires an annual self-assessment of cybersecurity measures.

All companies that need this level of certification must follow the FAR 52.204-41, and focus on the protection of FCI.

LEVEL 2

ADVANCED

The second level is for companies working with FCI and Controlled Unclassified Information (CUI). It requires a tri-annual third-party assessment for critical national security information, and an annual self-assessment for other covered programs.

Companies handling CUI must follow the NIST Special Publication for Protecting CUI.

LEVEL 3

EXPERT

The third level is for companies working on the highest priority programs, along with CUI and FCI. The government will conduct tri-annual assessments, and you must follow the NIST Enhanced Security Guidelines for Protecting CUI.

INTELLIGENT TECHNICAL SOLUTIONS

WHAT LEVEL OF CMMC DO YOU NEED?

LEVEL 1

FOUNDATIONAL

- Handle Federal Contact Information (FCI)

LEVEL 2

ADVANCED

- Handle Federal Contact Information (FCI)
- Handle Controlled Unclassified Information (CUI)

LEVEL 3

EXPERT

- Handle Federal Contact Information (FCI)
- Handle Controlled Unclassified Information (CUI)
- Handle DoD High-Priority Programs

HOW DO I GET CMMC 2.0?

The time to complete CMMC 2.0 depends on the size and complexity of your organization. The process is more rigorous than CMMC 1.0, but it is a continuous assessment of your compliance efforts rather than a one-time review.

The following is roughly how it works:

1. Developing an IT survey plan and conducting surveys with key stakeholders
2. Analyzing results from surveys and other data sources (e.g., audits)
3. Review the specific guidelines for the level of accreditation you desire
4. Creating an action plan based on findings from surveys and key guidelines
5. Implementation of regulations and discovered points of improvement

After setting up your IT environment to follow CMMC guidelines, you must work with a third-party assessment organization (aka a C3PAO) that the CMMC Accreditation Body has approved. The C3PAO will assess your organization's cybersecurity practices and determine whether you meet the requirements for certification. If you are compliant, you will be granted a CMMC certification.

Before a C3PAO audits your IT environment, you must thoroughly assess your organization's cybersecurity practices and address any gaps or weaknesses before the C3PAO arrives to conduct the official assessment.

HOW MUCH DOES IT COST TO GET CMMC?

The cost of CMMC certification will vary depending on several factors, such as the size and complexity of your organization, the level of certification you are seeking, and the C3PAO you work with.

It's challenging to provide an exact cost without your organization's specific set up and desired goals.

The CMMC certification process generally involves several steps, including a self-assessment, an on-site assessment by a C3PAO, and any necessary remediation of any gaps or weaknesses in your cybersecurity practices. Each of these steps may have associated costs, such as fees for the C3PAO's services, the cost of implementing new cybersecurity measures, and any other expenses related to the certification process.

READY TO START YOUR CMMC JOURNEY?

At the end of the day, CMMC 2.0 is an important step towards establishing a cyber security program in any organization.

If you want to get your company CMMC accredited, you need IT experts to guide you through the process. As a Managed IT Service Provider with experience handling clients juggling multiple government regulations, we're offering a way for you to get a headstart on the process: a free cybersecurity assessment.

However, if you'd rather continue looking for more information about implementing cybersecurity regulations for your organization, check out our Learning Center.

Meeting the requirements of CMMC requires integrating multiple solutions. Depending on the extent of your security defense infrastructure, CMMC compliance may be a significant undertaking and expense to consider.

KEEP YOUR DOD CONTRACTS. PAINLESSLY.

Schedule a Meeting with us.

INTELLIGENT TECHNICAL SOLUTIONS

2880 Meade Ave #350
Las Vegas, NV 89102
Phone: (702) 605-6670
www.itsasap.com