Crowe

ARE YOU PREPARED?

Tips for helping you meet CMMC compliance

September 2021 | Webinar

Presenters

Tips for helping you meet CMMC compliance.

The CMMC framework can be challenging, but your organization can take proactive steps to address CMMC requirements. We'll show you how.

● **Christopher Wilkinson**

Principal,
Risk Consulting

● **Michael Del Giudice**

Principal,
Information Security and Data Privacy Consulting

A complex topic

Are you ready to navigate the CMMC landscape?

Learning the ins and outs of Cybersecurity Maturity Model Certification (CMMC) is critical for your organization to make the grade.

What is CMMC?

A standard implemented by the U.S. Department of Defense for organizations that have Controlled Unclassified Information (CUI).

Who does this affect?

Thousands of organizations in industries that include:

- Technology, Media, Telecommunications
- Manufacturing and Distribution
- Life Sciences
- Public Sector
- Healthcare

The time to act is now

Proactivity is the name of the game.

If you’re not determining how CMMC will affect your organization, you’re behind.

Why?

CMMC requirements will show up in **requests for information** and **requests for proposal** from the federal government.

If you are not certified by a third-party assessment organization (3PAO), then **you won’t be able to respond**.

Compliance is not an overnight process. Many organizations may need **new policies, procedures, and technologies to achieve compliance**.

A complex framework

Take your organization’s maturity to the next level.

> Based on our experience, the initial expectation is that most organizations will be targeting Level Three (“Good Cyber Hygiene”) for CMMC compliance.

MATURITY LEVEL	NUMBER OF CONTROLS
Level Five: **Advanced/Progressive**	All controls at Level Four 15 additional controls
Level Four: **Proactive**	All controls at Level Three 26 additional controls
Level Three: **Good Cyber Hygiene**	All of NIST 800-171 20 additional maturity controls ~ 120 total controls
Level Two: **Intermediate Cyber Hygiene**	55 total controls (48 from NIST 800-171)
Level One: **Basic Cyber Hygiene**	15 total requirements

A complex framework

Addressing NIST 800-171 previously doesn’t necessarily mean you meet all CMMC requirements.

The assessment of a CMMC practice or process results in one of three possible findings:

□ **MET**

□ **NOT MET**

□ **NOT APPLICABLE**

To achieve a specific CMMC level, contractors need MET or NOT APPLICABLE findings on all required CMMC practices and processes for both the desired level and all lower levels.

Don’t forget your third-party partners

Check to see if your inherited practices and process objectives meet CMMC requirements.

☒ If you can’t demonstrate adequate evidence for all assessment objectives, you will receive a **NOT MET** result for the practice or process.

☑ Evidence from enterprises or the entities should show inherited practices and process objectives are applicable to in-scope assets and that assessment objectives are met.

☑ For each inherited practice or process objective, a Certified Assessor will include statements indicating how they were evaluated and where they were inherited.

The list is long

How much CUI does your organization have?

One of the biggest challenges your organization will face is identifying the type of CUI data you have, where it resides, and who has access to it.

Examples of CUI categories include:

- **Protected Critical**
- **Information Systems Vulnerability Information**
- **Vulnerability Information**
- **Operations Security**
- **General Privacy**
- **Health Information**
- **General Procurement and Acquisition**
- **Federal Taxpayer Information**

Source: https://www.archives.gov/cui/registry/category-list

So, what can your organization do?

Here are some ways you can prepare.

5 steps to help you prepare for

CMMC compliance

01 Define your environment

02 Build your architecture

03 Take the pretest

04 Close your gaps

05 Take the certification test

01 Define your environment

How much CUI does your organization have?

CMMC compliance begins with understanding all the locations, systems, and personnel that contain or access CUI and Federal Contract Information (FCI) data that is in scope for certification.

If you don’t know where the data is, or you don’t have a plan or strategy, it’s easy to make a mistake.

02 Build your architecture

Reducing the systems and accounts with access can make certification smoother.

CMMC assessment methodology follows a data-centric security process that applies practices and processes equally, regardless of a contractor’s size, constraints, or complexity. All CMMC levels are achievable by small, medium, and large contractors.

To help manage the scope, systems storing or accessing CUI data can be secured on isolated network segments, which reduces the systems required to meet CMMC standards. Cloud solutions also can help you achieve isolation.

03 Take the pretest

Understanding your current gaps will create a stronger remediation strategy.

The CMMC pretest can help your organization identify existing gaps that need to be remediated in order to become certified.

04 Close your gaps

You can use a gap assessment to build your project timeline.

Based on the results of the pretest assessment, a mitigation strategy can be created depending on the volume and complexity of the gaps identified.

Results don’t typically happen overnight. Depending on the project, your time frame could last 12-18 months.

04 Close your gaps

Determine the gaps that you can close internally vs. those that need help from an outside provider.

Technology solutions that can decrease the burden on your team and decrease likelihood of non-compliance include:

1. Security Information and Event Management (SIEM) and Endpoint Detection and Response (EDR) solutions
2. Computer-based training solutions
3. Multifactor authentication

05 Take the test

When you’re ready, it's time to see if your organization meets CMMC compliance.

Control interpretations and requirements can be challenging and complex during the certification process. Your organization may want to use an experienced firm with deep cybersecurity knowledge to help evaluate your environment.

Once gaps are remediated, your organization can seek certification by an authorized firm that is approved to perform a CMMC certification assessment.

It’s a lot to accomplish

You don’t have to take the CMMC journey alone.

We have a wealth of subject-matter specialists who understand the CMMC framework, the requirements, and how you can make your compliance journey more successful.

Gap Assessments

We have extensive experience performing gap assessments against the relevant industry standards and can provide recommendations to address identified gaps.

Managed Detection and Response

We can help satisfy detection and response requirements for organizations that need to meet Level 2 or greater.

Cloud Design and Implementation

We can help identify and implement controls within a cloud environment to achieve compliance.

CMMC Compliance Accelerator

Crowe has a compliance solution that will provide you with a customized package of solutions to accelerate compliance.

Presenters

We are ready to help you with your CMMC challenges.

Christopher Wilkinson
Principal,
Risk Consulting
Christopher.Wilkinson@crowe.com

Michael Del Giudice
Principal,
Information Security and Data Privacy Consulting
Mike.DelGiudice@crowe.com

Reach out to schedule a consultation.

Crowe

Thank you

Smart decisions. Lasting value.™

Learn more at crowe.com

“Crowe” is the brand name under which the member firms of Crowe Global operate and provide professional services, and those firms together form the Crowe Global network of independent audit, tax, and consulting firms. “Crowe” may be used to refer to individual firms, to several such firms, or to all firms within the Crowe Global network. The Crowe Horwath Global Risk Consulting entities, Crowe Healthcare Risk Consulting LLC, and our affiliate in Grand Cayman are subsidiaries of Crowe LLP. Crowe LLP is an Indiana limited liability partnership and the U.S. member firm of Crowe Global. Services to clients are provided by the individual member firms of Crowe Global, but Crowe Global itself is a Swiss entity that does not provide services to clients. Each member firm is a separate legal entity responsible only for its own acts and omissions and not those of any other Crowe Global network firm or other party. Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global.

The information in this document is not – and is not intended to be – audit, tax, accounting, advisory, risk, performance, consulting, business, financial, investment, legal, or other professional advice. Some firm services may not be available to attest clients. The information is general in nature, based on existing authorities, and is subject to change. The information is not a substitute for professional advice or services, and you should consult a qualified professional adviser before taking any action based on the information. Crowe is not responsible for any loss incurred by any person who relies on the information discussed in this document.