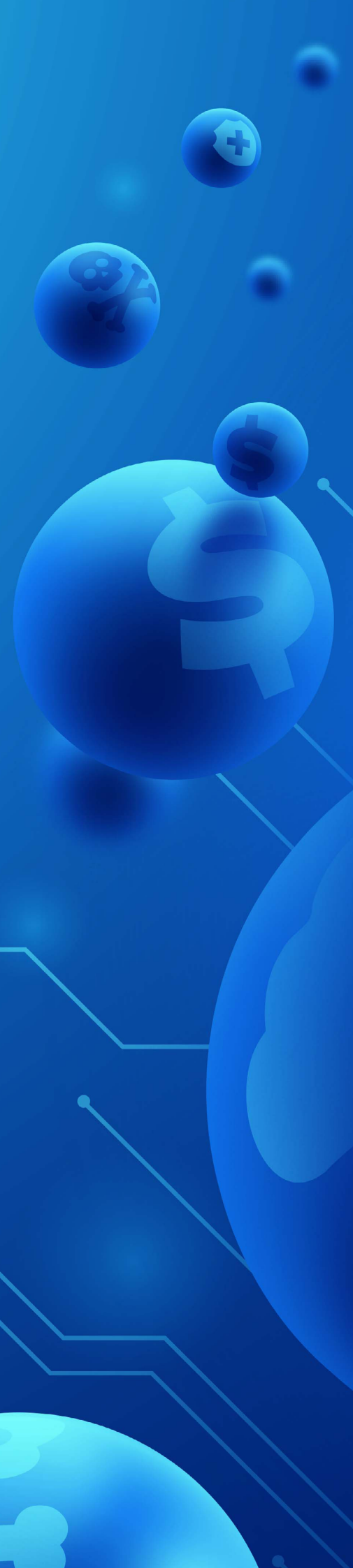




# Understanding the Cybersecurity Maturity Model Certification (CMMC)

---

FEBRUARY 2022



Obtaining a cybersecurity certification for your organization isn't just about checking a box to show you're following some best practices. Instead, it can thoroughly improve your organization's security posture if you follow through on these practices.

One such certification that's been getting attention lately is the [Cybersecurity Maturity Model Certification \(CMMC\)](#) from the U.S. Department of Defense (DoD).

This certification is often important for enterprises that want to contract or subcontract with the DoD. But it can also be something to follow as part of improving your organization's ability to work with sensitive information.

In this article, we'll walk through the details of the CMCC and show you how Kovrr can help you obtain this type of certification by providing financial quantification that can help you understand cyber risks so you can then strengthen your cybersecurity.

## What Is the Cybersecurity Maturity Model Certification (CMMC)?

The Cybersecurity Maturity Model Certification (CMMC) is a program from the DoD that certifies whether organizations have sufficient cybersecurity protections to be contractors and subcontractors for the Department.

"At a tactical level, the primary goal of the certification is to improve the surety and security of Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) that is in the possession and use of their federal contractors," [explains Varonis](#), a data security and analytics software provider.

But it also may be worth thinking about the CMMC as a general guidepost for those who do not work with the government but still want to ramp up their cybersecurity protections.

## Key Features of the CMCC

The certification is in the midst of changing from CMCC 1.0 to CMCC 2.0, so it's important to realize that some of the previous specifics of the certification are in flux. That said, the CMCC is still essentially rooted in making sure organizations follow cybersecurity best practices. In particular, the CMCC follows standards from the NIST (National Institute of Standards and Technology).

More specifically, the CMCC framework uses a tiered model, with different certification levels corresponding with more robust cybersecurity practices. Organizations that want to achieve this certification, at a level that corresponds with the protections needed for the information they may be accessing while working with the DoD, will need to pass assessments.

“CMMC 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,” [explains Amazon Web Services \(AWS\)](#).

## CMCC 2.0 vs. CMCC 1.0

For those somewhat familiar with CMCC 1.0, it’s important to recognize that the DoD is implementing CMCC 2.0. While the two are similar, some of the more notable changes include:

- + Moving from five levels of compliance down to three for CMCC 2.0
- + Aligning with NIST standards for CMCC 2.0 rather than having some standards that only apply to this certification
- + Enabling self-assessments for Level 1 and in some cases Level 2 for CMCC 2.0
- + Providing more “oversight of professional and ethical standards of third-party assessors,” [as the DoD notes](#).
- + Allowing for more flexibility and collaboration for certification

## When Will CMCC Take Effect?

Because CMCC 2.0 is still in the works, the DoD notes that organizations generally do not need to receive this certification to get a contract with the Department. Some pilot contracts included initial requirements, but [as the DoD states](#), “The Department does not intend to approve inclusion of a CMMC requirement in any contract prior to completion of the CMMC 2.0 rulemaking process.”

That process can take 9-24 months, according to the DoD.

## How Does Kovrr Help With CMCC Compliance?

Kovrr’s Quantum cyber risk quantification platform helps enterprises to financially quantify cyber risk on demand, which can play a significant role when it comes to complying with several key NIST requirements that are required for obtaining the CMCC 2.0.

For example, Level 2 of CMCC 2.0 matches the security practices of NIST Special Publication 800-171. That publication includes areas like “Security Assessment”, where organizations take actions like reviewing their security controls periodically and developing/implementing plans to fix deficiencies.

By working with [Kovrr's financial quantification output](#), a manager can immediately know where their most significant financial exposures for cyber events exist. From there, they can develop a security plan that addresses these exposures. And since the tool can be run on-demand, users can continually see where they stand and how they should prioritize new security gaps that emerge. Understanding the financial implications makes it easier to calculate ROI and can help organizations allocate their security budgets accordingly.

Another area of this NIST Special Publication that Kovrr aligns with is “System and Communications Protection.”

In this domain, organizations look at areas like their communications systems and how they're protecting sensitive information. Kovrr can help define security requirements that are based on measured goals. And by coming up with a [quantitative figure](#) for the overall exposure, it's easier to communicate with different stakeholders about cyber risk without necessarily having to divulge the details of what these risks are in a way that would expose sensitive information.

[Financial quantification](#) can also inform areas like “Awareness and Training”, as organizations may want to design their security training programs in a way that prioritizes protecting their most valuable assets. With quantum modeling, companies can focus on reducing their exposure to the scenarios that will cause the more severe impacts.

Altogether, Kovrr can help organizations more efficiently understand their [cyber risk](#) and spot potential financial impacts they may have not understood before. Enterprises can use the financial specificity that the platform provides to design their security practices in ways that will help them obtain the CMCC. And even if they're not looking to get this certification, Kovrr can simply be used to improve their cybersecurity.

**Want to see how Kovrr's financial modeling can help improve your security practices? [Book a demo](#) with our experts.**

## The Author



Shalom Bublil

CPO

---

## About Kovrr

Kovrr's cyber risk modeling platform delivers global (re)insurers and enterprises transparent data-driven insights into their cyber risk exposures. The Kovrr platform is designed to help chief risk officers, chief information security officers, underwriters, exposure managers, risk professionals and catastrophe modelers understand, financially quantify and manage cyber risk by utilizing AI-powered risk models. To learn more please contact the Kovrr team: [contact@kovrr.com](mailto:contact@kovrr.com)