CMMC Insights from Kloud9IT

What is Cybersecurity?

In simple terms, cybersecurity is the application of technologies, processes and controls to protect systems, networks, programs, devices, and data from cyber attacks[1]. Cyber attacks are no longer a rarity, and such attacks have made their impact known on both small and large scales. Should you fall victim to one, these attacks can put an entire enterprise out of business and leave a whole government, and its population, vulnerable to foreign entities.

What is CMMC?

CMMC stands for Cybersecurity Maturity Model Certification and it is just that: a certification. Contrary to the widespread belief, CMMC is NOT a cybersecurity framework.

It is a U.S. Department of Defense (DoD) program that applies to Defense Industrial Base (DIB) contractors[2]. It is a unifying standards to ensure that sensitive information is properly protected.

Why is CMMC Needed?

To be clear: Not every enterprise or business needs to be CMMC certified. CMMC is required of any member of the DIB that has DFARS 252.204-7012 contractual requirements. This includes contractors who interact exclusively with the DOD and all subcontractors as well[3].

In short, this means enterprises and businesses that deal with controlled unclassified information must be compliant. Examples of such would be manufacturers, universities, research institutions, consulting companies, and service providers.

1 https://www.itgovernance.co.uk/what-is-cybersecurity#:~:text=Cyber%20security%20is%20the%20application,systems%2C%20networks%2C%20and%20technologies

2 https://www.cisco.com/c/en/us/products/security/what-is-cmmc.html

3 https://www.cybersaint.io/glossary/who-needs-to-comply-with-cmmc#:~:text=CMMC%20is%20required%20of%20any,and%20any%20and%20all%20subcontractors

KLOUD9

To obtain this certification, the NIST800-171 must be implemented. The NIST 800-171 is a cybersecurity framework that outlines the required security standards and practices for non-federal organizations that handle CUI (Controlled Unclassified Information) on their networks[4].

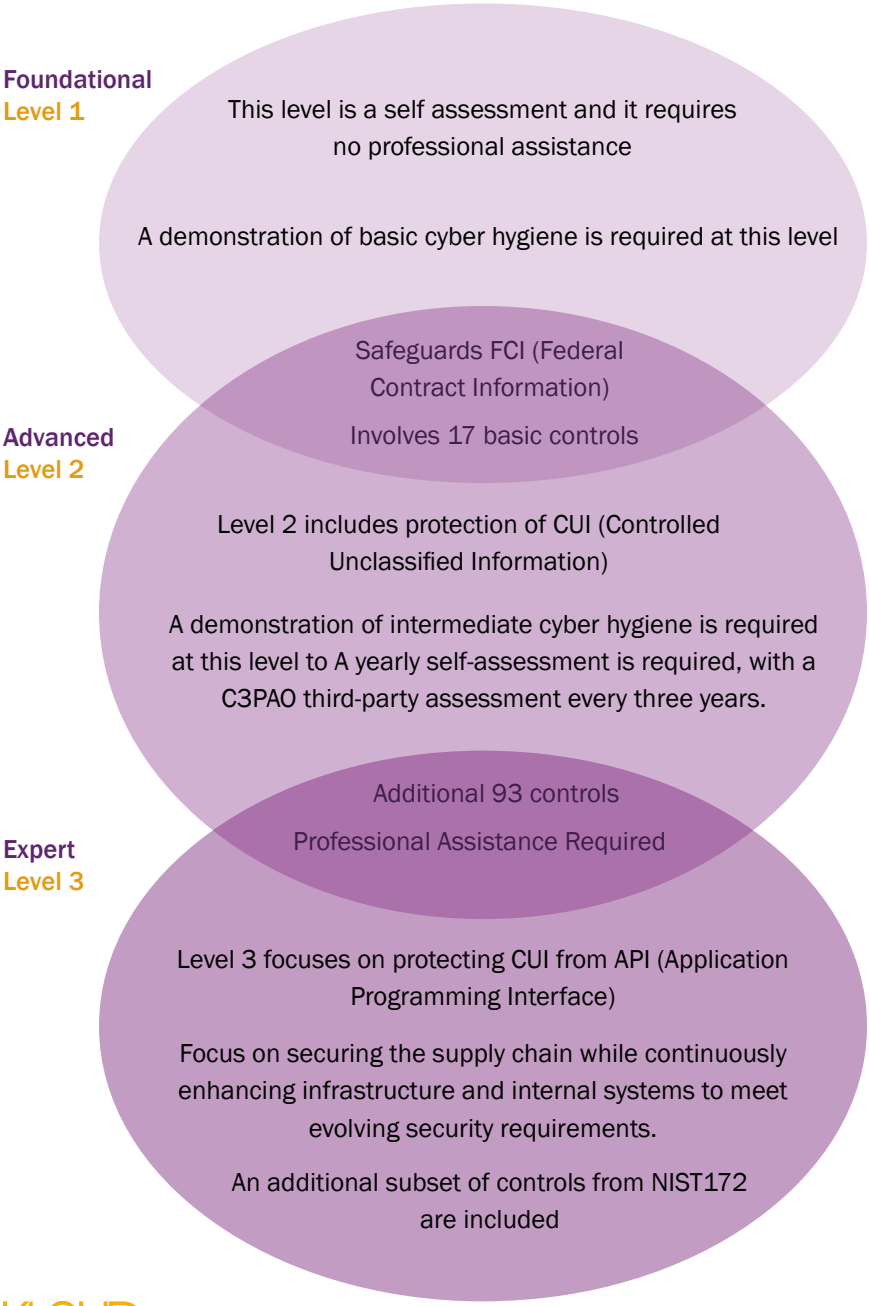
CMMC Simplified

There are 3 levels to CMMC and there are 3 safeguard types that CMMC covers. Each of these levels and safeguards overlap and build off one another, which is why having a base-level understanding of CMMC is critical.

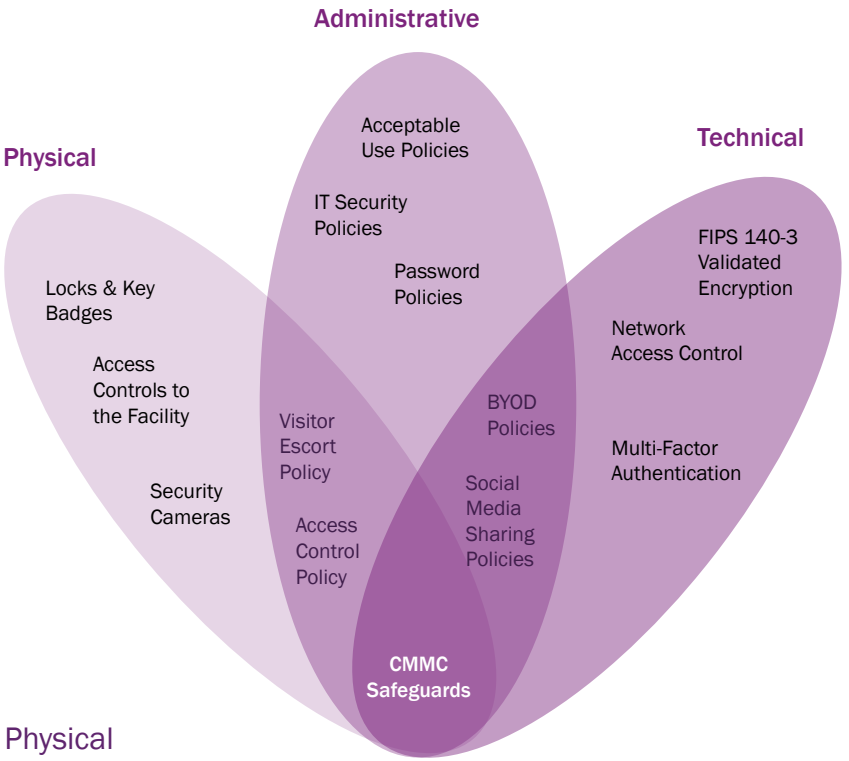
The three levels start at the Foundational level (Level 1), move up to the Advanced level (Level 2), and then end with the Expert level (Level 3). The 3 types of safeguards covered by CMMC are Physical, Administrative, and Technical.

4 https://www.titania.com/resources/guides/nist-800-171/#:~:text=NIST%20800%2D171%20is%20a%20publication%20that%20outlines%20the%20required,handle%20CUI%20on%20their%20networks

CMMC Levels



KLOUD 9



Physical

Involves the physical protection of CUI. Physical Protection activities ensure that physical access to CUI asset containers is strictly controlled, managed, and monitored in accordance with CUI protection requirements[1].

Administrative

Involves administrative actions, policies, and procedures. Administrative Protection policies are the precise set of instructions on how to carry out security actions, and it is important to be certain that they are not overlooked.

Technical

Involves the technological protection of CUI. Technical Protection measures can be very diverse as its scope ranges from security testing, auditing of online activity, access control, and making sure all software is updated and working properly[2].

1 https://www.pivotpointsecurity.com/cmmc-physical-protection-domain-heres-the-nitty-gritty/

2 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7122347/

KLOUD 9

CMMC
Culture Modification & Managing Change

Implementing the NIST 800-171 cybersecurity framework implies more than simply having your IT department “do it.” A traditional IT department specializes in the administration and application of hardware and software, whereas cybersecurity revolves around information control. Therefore, a business will need to undergo various changes to its structure to ensure adequate compliance.

Culture Modification

Since this framework encompasses more than just technical aspects, as seen in the previous text, it will take more than just an IT department to ensure that an organization stays compliant. It will involve a company-wide culture shift that will affect everyone in the organization.

The modification starts with the C-suite. Those higher up in the company must create specific and detailed policies that outline what behavior is acceptable/unacceptable.

It then becomes managements’ role to properly see that these new policies are enforced. Failure to enforce these policies could lead to a data breach and serious consequences.

Lastly, it is the job of employees to see that they follow these new policies and report anyone that is not following them properly.

Managing Change

Managing this change can be challenging, but not impossible. But there are a few key steps to always consider:

- Explain the need for these changes to all company employees in detail so that it is understood why there will be new policies and procedures in place
- Provide in-depth training on how to follow/carry out these new policies to help make the transition as smooth as possible
- Assign or hire a CISO (Chief Information and Security Officer) whose role is to focus on data protection, IT and infrastructure security, and maintain the company's cybersecurity strategy
- Obtain a subject matter expert, separate from the CISO, to help avoid common mistakes and ensure appropriate and compliant actions

CMMC at Kloud9IT

Staying compliant doesn't happen overnight. It can take a while to craft these intricate policies and to ensure they are being enforced. There are many other obstacles that may get in the way, such as employees being resilient to change or businesses growing and expanding into new territories.

At Kloud9IT, we understand that implementation is a journey without a fixed ending. That is why we treat CMMC as a cyber program, instead of in a "checklist" fashion. We designed our approach to CMMC to be as thorough and strategic as possible so that your company can become CMMC certified and stay compliant.

The Kloud9IT Difference

- Our compliance team holds various certifications in the realm of CMMC and go beyond what is required for consulting
- Kloud9IT treats compliance as a journey rather than a destination
- Being an MSP, we are capable of taking care of the technical safeguards
- We guide you throught every step of the implementation process
- Our dedicated team will meet with you on a regular basis

Contact Us Today for Your CMMC Needs:

Call

1-844-556-8394 x810

or schedule an appointment at

https://go.appointmentcore.com/guest/book/2yyWVJ

KLOUD 9

Kloud9IT Testimonials

WE PASSED CMMC JSVA!

Passing the JSAV audit was a major milestone for our organization—and we couldn't have done it without the incredible support from our IT partner. Their expertise, responsiveness, and proactive approach played a key role in helping us meet the rigorous standards required.

This achievement reflects not only our commitment to security and compliance but also the strength of our partnership. We highly recommend their team to anyone looking for a reliable, knowledgeable, and strategic IT ally.

*Due to compliance requirements, company name can not be shared

CONGRATULATIONS KLOUD9!

CONGRATULATIONS Kloud9 on your successful Cybersecurity Maturity Model Certification ("CMMC") certification and perfect 110-point Supplier Performance Risk System ("SPRS") score! It was a pleasure to support you on your CMMC journey!

Despite multiple "strategic pauses" and some other headwinds, CMMC requirements will likely start showing up in contracts with the United States Department of Defense ("DoD") before the end of this calendar year. Some DoD contractors have already made the strategic decision to start their CMMC journeys, positioning themselves ahead of their competition.

While on their CMMC journey, many companies find that it is more efficient and cost-effective to have an external service provider manage their IT and cybersecurity programs. The problem those companies face is that many managed IT and cybersecurity companies are deciding that they won't help clients meet the CMMC program requirements. Other external service providers claim to know how to get their clients ready but have yet to have a single client undergo a CMMC assessment.

That's what makes Kloud 9's CMMC certificate so momentous. Kloud 9 isn't just learning on the job while their clients take all the risk. Instead, they have invested in training their staff and earning a CMMC certificate for their own environment. As one of the first external service providers in the world to earn a CMMC certification, this positions Kloud 9 as a leading provider of managed services to defense contractors across the nation.

- Fathom Cyber

KLOUD 9

Kloud9IT's CMMC Insight