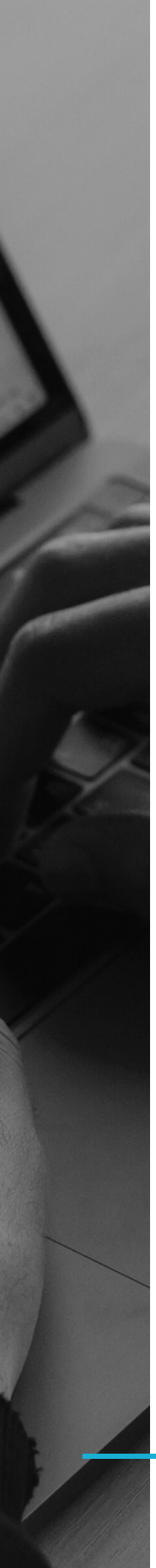
Cybersecurity Maturity Model Certification:
What You Need to Know

Whitepaper

2023

AGILEBLUE



INTRODUCTION TO CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

Cyberattacks on governments have skyrocketed in recent years, calling for more cybersecurity measures to be implemented by government contractors and departments. Cyber criminals are finding more vulnerabilities in government networks and clouds leading to concerns of increasingly severe cyberattacks in the future. These cyberattacks have also led to large financial losses for government agencies as they attempt to restore confidential data, networks and clouds. The introduction of the Cybersecurity Maturity Model Certification (CMMC) plans to secure clouds and networks that store sensitive government data. These standards will guide contractors and give them a solid foundation for cybersecurity. The Department of Defense (DoD) has introduced this model with the goal that their contractors and suppliers will operate in a more secure digital environment. By using pre-existing requirements like NIST and AIA, they hope to strengthen the cybersecurity posture of contractors. This new standard also provides contractors and suppliers with the opportunity to improve their cybersecurity practices through a system of levels. While CMMC only applies to the federal government right now, it serves as an example to other industries, like healthcare, who hope to standardize their cybersecurity in the coming years.

This whitepaper breaks down the basics of the CMMC guidelines for DoD contractors and suppliers and highlights the importance of cyber hygiene on each level of requirements. It's important that these standards are closely followed and that the proper practices and procedures are put in place in order to achieve maximum cybersecurity on each level. There is also a chart featured that explains each level and the steps that must be taken in order to achieve them. We also break down who is most affected by the implementation of CMMC and how to get started integrating security practices into everyday operation. Overall, this whitepaper serves as a guide for you to become acclimated with the new CMMC standards and to help you implement these guidelines into your own contract and supplier roles.

What is CMMC?

The Cybersecurity Maturity Model Certification (CMMC) was created by the Department of Defense (DOD) at the beginning of 2020 to ensure the highest standard of cybersecurity when working with confidential information. In the past, government contractors and suppliers have self-regulated their cybersecurity precautions leaving room for error and gaps in their networks. The CMMC provides a more formal model for cybersecurity requirements and removes the possibility for human error. It also provides added security for Controlled Unclassified Information (CUI) that is usually vital to government agencies.

The CMMC defines a contractor's cybersecurity maturity based on five levels that rank their cybersecurity from "Basic Cyber Hygiene" to "Advanced/ Progressive Cybersecurity." Within each level are a list of practices that correlate with each level. In addition, there are 17 domains that include practices relating to "Access Control", "Incident Response", "Situational Awareness", etc. Within each larger domain, there are smaller capability domains that must be met within each level. The principles of these domains include end-to-end encryption, encrypted logs, cloud-based services, controlled access, and key-based authentication. While contractors don't need to meet every capability domain, it's important that they remain mindful of what's required of them at each level.

WHY IS CMMC IMPORTANT?

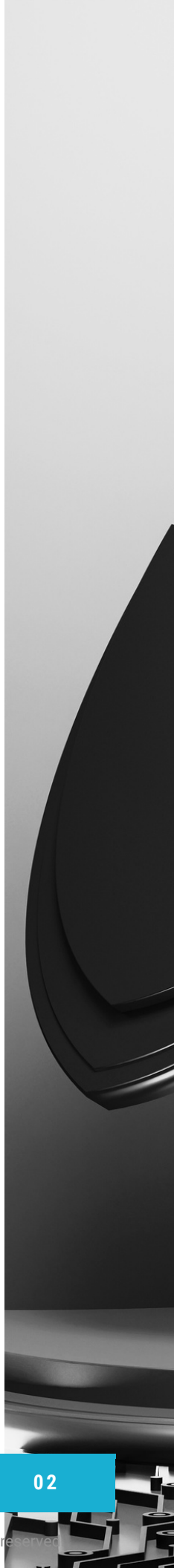
The impact of cybercrime costs U.S industries billions of dollars in damages each year along with the loss of important data and intellectual property. In 2022, the FBI received more than 800,000 cybercrime-related complaints, with losses totaling over $10 billion. While the government has started to invest in additional cybersecurity safeguards and implement new legislation regarding cybersecurity laws, the number of cyberattacks is still expected to be high due to quickly evolving technology. The introduction of the CMMC model is part of the plan to secure the networks and clouds of all government contractors who are at risk to being targeted by hackers due to the sensitive data with which they work. It also provides the DoD with cybersecurity consistency among their contractors and suppliers while they work on projects that range in the need for increased security.

The introduction of the CMMC model will serve as increased security for unclassified information from government agencies, which would otherwise have the potential to be easily accessed by cyber criminals. This unclassified information includes Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) which are both common forms of data that DoD contractors use when working on projects. The information relates to a range of government activities from Finance and Immigration to Defense and Natural Resources.

WHO DOES THIS AFFECT?

Starting in 2025, all new and current 300,000 DoD contractors and suppliers will need to obtain this certification if they want to continue working on projects for different government departments. These contractors should evaluate their current cybersecurity practices and identify any gaps in their processes. Once they meet all the CMMC standards they should not stop monitoring their security practices. They will also be subject to external cybersecurity assessments instead of the previous cybersecurity self-assessments in order to maintain more accountability.

The DoD will soon exclusively work with contractors who meet CMMC standards. This requirement will mean increased security for DoD and other connected departments. It will also provide increased protection for Controlled Unclassified Information (CUI) within DoD networks. As the DoD continues to work with new and existing government contractors in the future, they will have the ability to structure new contracts around CMMC guidelines and their cybersecurity levels.



CMMC 1.0

CCMMC 1.0 was the original model to improve cybersecurity in organizations working with the U.S. Department of Defense. It featured five levels, starting with basic cyber hygiene and progressing to advanced capabilities. Each level included specific security controls. It aimed to standardize cybersecurity practices for DoD contracts based on the sensitivity of handled information and was eventually replaced by CMMC 2.0.

CMMC 2.0

CMMC 2.0 introduces notable changes to the Cybersecurity Maturity Model Certification (CMMC) standards. The most prominent alteration is the introduction of a multi-level framework that offers greater flexibility and scalability for organizations. This framework comprises three levels: Beginner, Advanced, and Expert. The Beginner level allows for annual self-assessments and is tailored for organizations just starting on their cybersecurity journey. The Advanced level, which replaces the original CMMC Level 3, focuses on aligning with NIST SP 800-171 and mandates triannual third-party assessments for critical national security information. The Expert level, a new addition, demands over 110 practices based on NIST SP 800-172 and requires government-led assessments every three years.

Another significant change is the reduction in the number of security requirements from the original CMMC model. CMMC 2.0 drops certain security requirements while emphasizing practices aligned with NIST standards. These changes aim to make CMMC more adaptable and inclusive. Additionally, the introduction of government-led assessments at the Expert level strengthens security assurance, emphasizing the protection of critical national security information. Overall, CMMC 2.0 aims to strike a balance between cybersecurity rigor and practicality, allowing organizations to tailor their compliance efforts according to their maturity and the sensitivity of the information they handle.

CMMC 1.0

Level	Requirements
Level 1 – Basic Cyber Hygiene	The lowest level of CMMC requires basic safeguarding practices for contractors to follow. For example, they must install anti-virus software, consistently change and create secure passwords, and control access to sensitive information.
Level 2 – Intermediate Cyber Hygiene	Controlled Unclassified Information (CUI) is largely protected under level 2 which includes, "any information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls." Contractors are also required to establish and document their practices.
Level 3 – Good Cyber Hygiene	Along with the guidelines from previous levels, complying with NIST standards and securing CUI all apply to level 3. Organizations are required to establish and maintain a cybersecurity plan under this level.
Level 4 - Proactive	Most cybersecurity standards are met at this level, so processes for reviewing and measuring the effectiveness of cybersecurity practices are ensured. A continuation of CUI protection and NIST standards are also followed at this level.
Level 5 – Advanced/ Progressive	After achieving the highest level, contractors should have strong cybersecurity standards implemented across the organization along with additional advanced strategies that detect and respond to Advanced Persistent Threats (APTs).

CMMC 2.0

Level	Requirements
Level 1 – Foundational	The new "Level 1" comprises 17 practices and permits organizations to conduct annual self-evaluations. This beginner-level assessment enables organizations to assess various aspects, such as staff, IT systems, existing controls, and unimplemented processes.
Level 2 – Advanced	The "Advanced" level in CMMC 2.0 reduces security requirements by 20 compared to the original model but introduces 110 security practices aligned with NIST SP 800-171. While annual self-assessments are required for some programs, organizations aiming for compliance with this level must undergo triannual third-party assessments for safeguarding critical national security information. Achieving compliance with CMMC 2.0 Level 2 signifies an organization's ability to securely handle Controlled Unclassified Information (CUI).
Level 3 –Expert	The "Expert" level mandates over 110 practices aligned with NIST SP 800-172, akin to the Advanced level. It includes a few additional practices and controls. However, what distinguishes the Expert level is that it necessitates triannual government-led assessments and does not accept self-evaluations or third-party assessments as sufficient for compliance.

CMMC Capability Domains

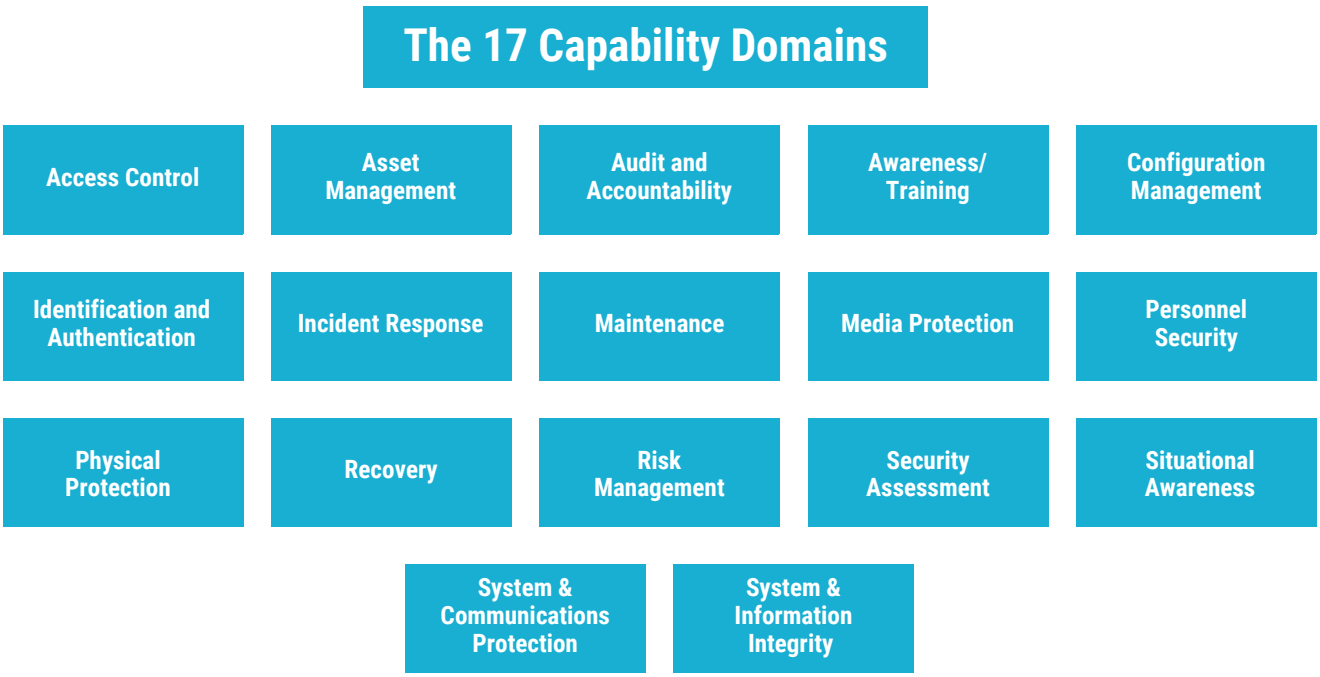
For organizations looking to work towards CMMC 2.0 compliance, the 17 CMMC Capability Domains are a vital framework. They offer a clear roadmap for improving an organization's cybersecurity measures and achieving regulatory compliance.

These domains cover a wide range of critical cybersecurity areas, including access control, asset management, incident response, and risk management. This comprehensive coverage ensures that organizations are addressing all aspects of cybersecurity effectively.

Moreover, the practices and requirements within each domain are tailored to an organization's specific circumstances, considering factors like maturity level and data sensitivity. This means organizations can take a targeted approach to compliance, focusing on what's most relevant to their operations.

By achieving compliance across these domains, organizations not only meet regulatory requirements but also bolster their overall cybersecurity resilience. This enhances their ability to protect sensitive data and systems, mitigating the risks of cyber threats and incidents.

In summary, the 17 CMMC Capability Domains provide organizations with a structured and adaptable framework to guide their journey towards CMMC 2.0 compliance, ultimately strengthening their cybersecurity posture and safeguarding critical information.



HOW TO GET STARTED:
WORKING TOWARDS COMPLIANCE

CMMC standards are not optional for government contractors, so it's important that you seek additional guidance if you're unclear of all of the requirements. The first step is to understand which level your organization or project falls under. From there, it's important that you fully understand what is required to move forward. If you find that you are a Level 3 or higher, you'll need must have log monitoring and log correlation as NIST standards have a detect and response section that they must adhere to.

As the levels increase, the more complicated the requirements become. If your organization does not have an in-house Security Operations Center (SOC), consider referring to experts to help you identify any gaps you may have. AgileBlue is a managed breach protection with an AI-Enabled SOC|SOAR platform. We provide the support you need when aiming to complete your certification by keeping you compliant for Levels 3 and higher. AgileBlue protects your network, cloud and endpoints with vulnerability management, continual monitoring, and intelligent analysis. With our cyber risk scoring algorithm, we can show your risk gaps in real-time. Our Silencer technology reduces false positives with a 95% confidence score. With automated threat monitoring, we can detect threats faster in real-time. CMMC assessments are also available to help identify the best methods for getting started.

As professionals move along in the process it's important that they document their practices and procedures during the compliance process. It can initially be a steep cost for contractors to meet CMMC standards at first, but it should be viewed as an investment that can prevent them from paying a much higher ransom should they be targeted by cyber criminals. They should also plan to continue implementing different practices as they move up in the levels of requirements.

AGILEBLUE

AgileBlue Cerulean combines the power of AI-enabled cybersecurity with the human touch you trust. Our SOC|SOAR platform is designed to quickly and accurately detect cyber threats across your entire digital infrastructure and cloud, providing you with 24/7 monitoring, detection, and response. AgileBlue's innovative Cerulean platform is custom fit to your company, so you not only get the best technology on the market, but you get the perfect fit, for your specific needs.

Ready to start protecting your company?

REQUEST A DEMO