DoD Cybersecurity Maturity Model Certification (CMMC)

A Guidehouse Perspective
The Defense Industrial Base (DIB) is Vulnerable

The theft of intellectual property and sensitive military and defense information due to exfiltration poses an existential threat to the national and economic security of the United States and compromises our military’s warfighting superiority. With the acknowledgment in the Department of Defense (DoD) 2018 National Defense Strategy that cyberspace is a warfighting domain, the Department has continued to prioritize defending DoD systems and networks from malicious cyber actors. As the DoD’s supply chain and reliance on defense contractors has continued to expand, so has the realization that the Defense Industrial Base (DIB) is the soft underbelly of the Department’s cybersecurity posture.

DoD Challenge

As the exfiltration of covered defense information (CDI) from DIB partner networks has increased in both scale and severity, DoD has struggled to issue and implement effective guidance to the DIB to control and contain the problem.

In 2016, DoD issued the Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, requiring DoD contractors to safeguard CDI based on controls outlined in NIST SP 800-171, and requiring the reporting of cyber incidents. While this was a good first step, it only required that companies self-attest to compliance with these standards. Many DIB companies struggled to plan for and implement these required controls. A 2018 MITRE report found the vast majority of government contractors were not meeting the requirements of DFARS 7012, and many more did not have an understanding or capability to meet the criteria for the contract.²

CMMC is Born

In late January 2020, DoD released the Cybersecurity Maturity Model Certification (CMMC) as a unified cybersecurity standard for future DoD acquisitions. The CMMC shares the goal of the CDI DFARS clause to reduce the exfiltration of controlled unclassified information (CUI) from the DIB and protect data on DIB partner networks and is based largely on the set of security controls in NIST SP 800-171. CMMC adds the requirement for DIB companies to be assessed and certified by an approved 3rd party auditor. The intent is for this certification step to be a forcing function to promote and enhance the cybersecurity posture of the DIB by requiring contractors to demonstrate that they meet the required security controls, and to give the government better visibility and awareness of the DIB’s cybersecurity posture.

CMMC will be a mandatory requirement for all companies doing business with the DoD. Certification is required for both prime and subcontractors. DoD will begin including the CMMC clause out in new Requests for Information (RFIs) starting in June of 2020, and in Requests for Proposal (RFPs) in the fall of 2020.

---

CMMC measures and assesses maturity of both processes and practices of security controls across 17 capability domains and 43 capability areas and pulls most of its requirements from existing controls in FAR Clause 52.204-21 and NIST SP 800-171. CMMC is not a one-size-fits-all model; the framework has five (5) levels of maturity from basic safeguarding to protection against Advanced Persistent Threats (APT). This is intended to ensure CMMC requirements are not overly burdensome on small to mid-size businesses that may not have the resources to implement more advanced cybersecurity protection measures. Future solicitations will define the required level of maturity based on the sensitivity of information and the level of safeguarding required.

**CMMC Model Structure**

<table>
<thead>
<tr>
<th>Processes</th>
<th>Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>Level 1</td>
</tr>
<tr>
<td>Level 2</td>
<td>Level 2</td>
</tr>
<tr>
<td>Level 3</td>
<td>Level 3</td>
</tr>
<tr>
<td>Level 4</td>
<td>Level 4</td>
</tr>
<tr>
<td>Level 5</td>
<td>Level 5</td>
</tr>
</tbody>
</table>

- **Level 1**: Performed, Basic Cyber Hygiene
- **Level 2**: Documented, Intermediate Cyber Hygiene
- **Level 3**: Managed, Good Cyber Hygiene
- **Level 4**: Reviewed, Proactive
- **Level 5**: Optimizing, Advanced/Progressive

**17 Capability Domains**

- Access Control
- Asset Management
- Awareness & Training
- Audit & Accountability
- Configuration Management
- Identification & Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical Protection
- Recovery
- Risk Management
- Security Assessment
- Situational Awareness
- System & Communications Protection
- System & Information Integrity

*Figure 1: CMMC Model Structure*
Why Now?

With version 1.0 of the CMMC Framework officially published on January 31, 2020, there is a sense of urgency for companies to prepare for their CMMC assessment and certification, which will begin rolling out in fall 2020. Based on the type of work companies are engaged in today, and the type of work they endeavor to do, companies should prioritize identifying their desired CMMC level, and then work to identify their gaps, and what is needed to address them. By starting this process now, companies can ensure they have enough lead time to develop a comprehensive plan, identify and devote the necessary resources, and implement corrective actions in a thoughtful way that aligns with the work the organization is already doing as part of their broader IT strategy. There is a tremendous advantage for early adopters with the opportunity to pursue new DoD work before the competition is certified. Certification instantly improves corporate credibility with shareholders in the market, and the ability to attract and retain qualified staff.

Late adoption and insufficient planning can introduce unnecessary risk and can require significant resources downstream to address needed changes. Companies are often surprised at their existing level of compliance when measured against both the practices and processes required by the CMMC framework. Often, technical controls have been implemented, but the necessary policies and processes are not in place to ensure they are maintained and updated.

Companies tend to underestimate the required work needed to attain and maintain a given level of compliance. When efforts such as this are undertaken without the necessary planning time, required remediations are often made as stopgaps, but are not fully integrated into an organization's enterprise or security architecture. These tend to lead to costly investments or significant rework down the line. One of the worst possible outcomes of late adoption happens when companies only determine their level of compliance after a failed assessment. This can have a significant impact on the work an organization can compete for and win, potentially setting them back to square one in terms of certification preparation.
Guidehouse Approach

At Guidehouse, we understand that an organization’s CMMC needs will vary based on a variety of factors, including organization size, the maturity of existing cybersecurity programs, targeted CMMC level, and available resources. Guidehouse works closely with our clients to understand their specific needs and develop an approach that aligns with their timelines, resource constraints, and security goals. Our CMMC offerings are tailored to meet individual needs but are centered around three primary services to help organizations prepare for CMMC success.

For organizations looking to take the first step towards CMMC compliance, Guidehouse offers a Preparatory Assessment, where we assess your organization’s current state cybersecurity practices, processes, and controls and determine your current CMMC-level alignment. We then identify and document the gaps that exist to get to the desired level. Using automated tools to streamline data collection and dashboards, Guidehouse helps organizations visualize the gaps and key insights for leadership around areas of risk. These can be used to inform resource decisions around required cybersecurity investments. This assessment is a helpful first step to baseline what is needed to attain a desired CMMC level.

For organizations who may already be implementing NIST SP 800-171 or 800-53, or related controls on their internal networks, and feel confident they meet a given CMMC level already, our Preparatory Assessment can be a valuable exercise to validate that alignment, and to ensure all required documentation and processes are in place to support the official CMMC assessment. Many organizations have mature technical cybersecurity controls in place, but do not always have sufficient policies and processes implemented to ensure they are maintained and updated appropriately. If a self-assessment has already been completed, our assessment can be a cost-effective means to ensure an organization is audit ready.

Guidehouse can also develop a Remediation Strategy after our initial assessment that will identify specific processes, practices, and activities required to attain a desired CMMC level, including estimated costs and timelines, infrastructure upgrades, and policy and governance activities.

We work with your organization to confirm remediation activities are not treated as a checklist of needed fixes, but rather a suite of remediation options that align to your business needs, mission priorities, and cost and schedule constraints. Our cybersecurity experts are well versed in helping organizations implement effective cybersecurity controls holistically, using a risk-based approach.

Depending on your needs, Guidehouse has teams of qualified experts to help with the Implementation of the required controls identified in the remediation strategy and their integration into your cybersecurity program. We will work with IT and cybersecurity staff, senior leaders, and mission owners to ensure controls can be implemented to align with existing activities and without adversely affecting business operations.
Why Guidehouse?

Guidehouse brings a rich history of audit and cybersecurity assessment expertise supporting both federal and commercial clients. We have helped the DoD design and implement their audit and assessment programs and have assisted both DoD and commercial clients in implementing them. Our cybersecurity experts have long been involved in all aspects of the security controls CMMC is based on; from authoring policy for NIST; to helping oversee their implementation through senior executive positions within the Office of the Secretary of Defense (OSD); to our work assessing, auditing, and implementing CMMC-based controls for key U.S. government, DoD, civilian agency, and intelligence partners as part of the NIST Risk Management Framework (RMF), NIST SP 800-171, and financial management requirements processes.

Although CMMC requires specific controls be implemented to attain its certification, the security measures are not unique and should not be addressed or implemented in a vacuum. CMMC requirements should be integrated thoughtfully into an organization’s broader IT and cybersecurity program for maximum effectiveness from both a cost and a security standpoint. Guidehouse understands how to unite multiple stakeholder perspectives to achieve objectives that are not just compliant, but that align to and help accomplish business goals.

Capabilities

Guidehouse has extensive experience integrating IT strategy, cybersecurity, enterprise risk management, and data analytics into holistic programs for both commercial and government clients. Our approach brings together subject matter experts, luminaries, and business leaders from each of these areas to develop an integrated approach to addressing each of our client’s unique challenges. We understand the intricacies of DoD cybersecurity requirements and the unique challenges commercial entities face in implementing them.

Quality

Guidehouse has an impeccable reputation for quality and is the only professional services firm that has been recognized for the quality of its work by achieving NIST’s very own prestigious Malcolm Baldrige Award for Quality.

Experience

Guidehouse has experience across the federal landscape providing our commercial clients with an informed perspective to fully address CMMC requirements.

In support of a large Navy client who was charged with transitioning from DoD’s previous Certification and Accreditation (C&A) process to the RMF for over 66,000 users, Guidehouse provided the client with a detailed strategy, approach, and plan to implement over 900 security controls. We performed this assessment, provided a comprehensive Plan of Actions and Milestones (POA&M), and identified opportunities to take advantage of resource efficiencies, giving the client a cost-effective solution to implement the required security measures that was incorporated into their IT modernization strategy.
Guidehouse was instrumental in improving a classified Intelligence Community (IC) client’s information security program posture through the assessment, evaluation, and analysis of their cybersecurity program. We were the first external, independent Federal Information Security Management Act (FISMA) evaluator in the IC, building a maturity model-based evaluation aligned to requirements to provide clear guidance and ease of understanding of areas of improvement for the client. We designed and implemented an approach to assess key security controls across the agency, which we used to help determine the effectiveness of the information security program, and specific remediation activities in areas including Access Management, Risk Management, Configuration Management, and Continuity Planning. Our recommendations were then shared with the agency, IC-wide leadership, and Congress.

Guidehouse has years of experience baselining organizations’ cyber hygiene and providing strategic, managerial, and technical recommendations to guide the organizations towards a more secure, resilient cybersecurity program posture.

Additionally, for more than a decade, we have supported the Office of the Under Secretary of Defense (Comptroller), the DoD organization charged with oversight of Financial Management (FM) controls across the enterprise. Guidehouse helped develop and implement an audit readiness strategy that OUSD(C) implements across the Department. As part of this strategy, Guidehouse performed a risk assessment of the IT controls included in the Federal Information System Controls Audit Manual (FISCAM) and worked with the Government Accountability Office (GAO) to provide the Department a prioritized list of controls with the highest criticality for financial statement audits.

People

Guidehouse maintains a deep bench of highly qualified cybersecurity and audit readiness staff with not only the experience and expertise, but also the expert certifications recognized by DoD, including certified Certified Information Systems Auditors (CISAs), Certified Information Systems Security Professionals (CISSPs), and DoD Qualified Validators who not only understand the technical requirements, but also carry the contextual expertise to know how their implementation can impact broader organizational goals and resource constraints. Too often, vendors get lost in “by the book” implementations and fail to account for how decisions made in the present will impact the needs of organizations in the future. Our Cyber and DoD leadership teams include former commercial executives, DoD Senior Executive Service (SES), and military general officers with a deep understanding of how to successfully align business objectives with evolving cyber requirements.

With the CMMC framework published, and the requirement expected to be included in RFPs starting this fall, now is the time to prepare your organization for your CMMC assessment and certification. Ensure you understand the requirements, how your organization aligns today, and the time, resources, and cybersecurity activities needed to get you to your required level. Guidehouse is ready to help you understand your CMMC needs and develop a plan for success. Find out more by contacting us today at cybersecurity@guidehouse.com.
About Guidehouse

Guidehouse is a leading global provider of consulting services to the public and commercial markets with broad capabilities in management, technology, and risk consulting. We help clients address their toughest challenges with a focus on markets and clients facing transformational change, technology-driven innovation and significant regulatory pressure. Across a range of advisory, consulting, outsourcing, and technology/analytics services, we help clients create scalable, innovative solutions that prepare them for future growth and success. Headquartered in Washington DC, the company has more than 7,000 professionals in more than 50 locations. Guidehouse is a Veritas Capital portfolio company, led by seasoned professionals with proven and diverse expertise in traditional and emerging technologies, markets and agenda-setting issues driving national and global economies. For more information, please visit: www.guidehouse.com.