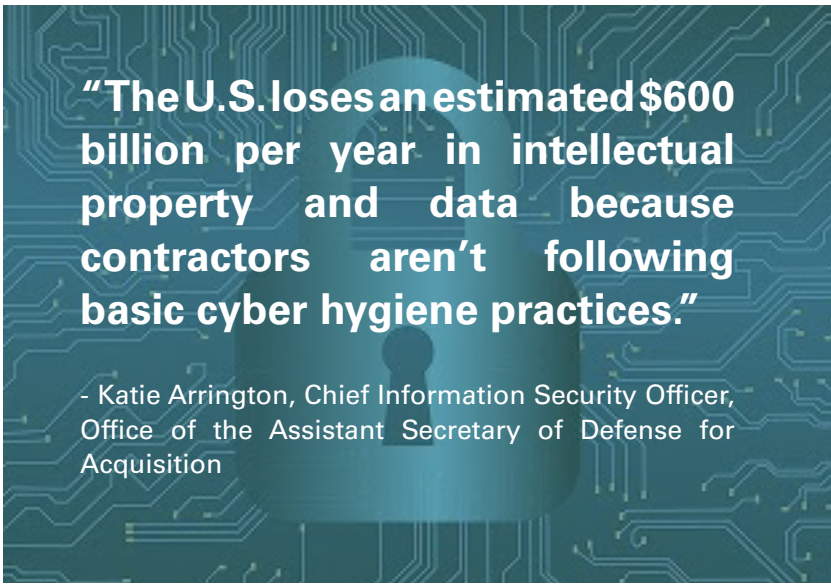
aronson LLC
ASSURANCE | TAX | CONSULTING
Expanding What's Possible

Cybersecurity Maturity Model Certification (CMMC)

Instilling a culture of cybersecurity awareness within an organization

Instilling a Cybersecurity Culture

Earlier this year the Department of Defense (DOD) announced the final version of the CMMC Model (v1.02). The Cybersecurity Maturity Model Certification (CMMC) consists of distinct security maturity levels (ML) ranging from "Basic Cybersecurity Hygiene" to "Advanced/Progressive". CMMC is intended for Defense Industrial Base (DIB) contractors who will be required to be formally certified using the CMMC model as a requirement for future contract awards. CMMC will eventually replace the current self-certification process that is mandated by DFARS 252.204-7012 and implemented via controls specified in NIST 800-171: Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and organizations.



In many of the discussions about CMMC, I find one thing lacking which is an emphasis on developing a culture of cybersecurity within DIB contractors and how that translates into reality for companies large and small. Achieving certification at any of the 5 CMMC maturity levels isn't just a one time or even triennial event (every 3 years) to demonstrate compliance with tens or hundreds of security practices to a certified 3rd party assessor (C3PAO). Businesses that think this way may be in for a rude awakening as they go through the initial assessments but even more so as the CMMC model evolves and becomes more complicated over time.

In fact, each CMMC maturity level consists of both practices (i.e. security controls) and processes as characterized in this figure.

Note: All references from CMMC Model V1.02 published March 18, 2020.

For example, CMMC ML 3 "focuses on the protection of CUI and encompasses all of the security requirements specified in NIST 800-171 as well as additional practices from other standards and references to mitigate threats". It is worth noting that all DOD contractors that process CUI have been required to self-certify compliance with all the NIST 800-171 standards since December 31, 2017. So in theory at least, for a DIB contractor that has already attested to meeting the NIST 800-171 standard, the bar to achieving CMMC ML 3 is fairly low.

Understanding Compliance

A lot of focus understandably has been on addressing the specific practices that are specified within the model in order to "pass" the assessment performed by an assessor. For example, CMMC ML 3 consists of 130 practices. However, CMMC ML 3 also requires processes that are "Managed" which "requires that an organization establish, maintain, and resource a plan demonstrating the management of activities for practice implementation. The plan may include information on missions, goals, project plans, resourcing, required training, and involvement of relevant stakeholders."

So while it is important to ensure that each practice is being conducted and followed within an organization, it is just as important to have a plan in place to demonstrate how the practice is being managed.

We'll use a relatively straightforward security practice to demonstrate our point. "Perform maintenance on organizational systems" is a required security practice (MA.2.111) at ML 2 and higher. These maintenance tasks range from applying appropriate software patches and updates to endpoints to ensuring a network device has the most up-to-date secure firmware version. It includes planned and unplanned maintenance, configuration changes, etc., performed on any hardware, firmware, or applications within your organization's boundary.

Most organizations will likely feel this is an easy practice to meet. However, it is not enough to "check the box" and tell an assessor "Yes, we perform system maintenance".

Here are some questions that you should consider:

- Does your organization have a record of the maintenance activities that have been performed over the past month, quarter, or year?
- Do you have a record of the systems that maintenance was performed on or what was involved in the last maintenance performed?
- Can you communicate what maintenance activities have been deferred and have you documented why or when those maintenance activities will be completed?

This is just 1 seemingly simple practice. Many practices are significantly more complex in demonstrating compliance as well as managing the processes related to that practice.

Cybersecurity and IT Operational Maturity

The security practice described previously demonstrates the interdependency between cybersecurity maturity and IT operational maturity. Large firms typically have the luxury of having dedicated staff for each separate but distinct function - IT operations (IT Ops) and IT security operations (SecOps). I would argue they are, on average, no more secure than the small to medium business (SMB) that has only IT Ops staff with little to no cybersecurity experience or capability. For example, in the case of Equifax breach, there was a known vulnerability that had been identified in a piece of software. But the team responsible for addressing the vulnerability didn't implement the fix for months. The result was that an attacker infiltrated their network and exposed the data of 147 million Americans. See CSO source article here.

Performing systems maintenance is typically the purview of the IT Ops function and not the SecOps function. But there are a lot of considerations that go into performing maintenance on a system. For example, the SecOps function will likely want to implement patches to critical systems right away to address existing vulnerabilities and potential security concerns. However, the IT Ops function may be reluctant to do so as it may cause unknown performance and application issues which will impact stakeholders. Here, both functions need to work in tandem to find the best approach while mitigating the risk appropriately.

Similarly, actions taken by the IT Ops function can have a negative impact on the overall security of an organization. A configuration change to a device or system may introduce a vulnerability. Or a change in hardware or software may require a re-assessment of how the organization addresses security practices that were dependent on that system. As such, the IT Ops function must be critically aware of its responsibilities as it relates to maintaining the security of the organization and must take into account cybersecurity considerations in its decision making.

Cybersecurity and Operations Maturity

The IT Ops function is just one stakeholder group that is also involved with meeting and demonstrating compliance with CMMC standards (along with SecOps function). However, there are actually multiple stakeholder groups within the organization that are also involved in achieving and maintaining compliance with CMMC practices. Here are a few of these groups:

Human Resources (HR) – The HR function is typically responsible for screening individuals interested in joining an organization (e.g. performing background checks). The organization has to trust that this screening process is consistently followed in order to demonstrate compliance with practices identified within the Personnel Security domain. Similarly, timely notification of personnel events (such as transfers and terminations) must be provided to IT in order protect organizational systems.

Facilities/Facility Security Officer (FSO) – The Facilities function or FSO is typically responsible for limiting physical access to a facility. This includes escorting visitors and monitoring visitor activity and maintaining logs of physical access to the facility. Demonstrating compliance with the practices identified within the Physical Protection domain will rely heavily on this function.

In addition to the above, your subcontract administrators, purchasing teams, and even employees themselves have responsibilities as it relates to maintaining the overall security of an organization.

A Culture of Security Awareness

It is impossible to have a secure and compliant IT environment without buy in and engagement from the entire organization. Here are some things to consider when evaluating your organization's readiness to undergo a CMMC assessment:

- **Is there buy-in from appropriate levels of management?** Tone from the top is crucial when implementing appropriate IT and security practices. If management leads the way in promoting a culture of security and risk awareness, it tends to resonate with employees. Communication, updates, and tangible actions by management supporting the mission and goals of IT Ops (and Sec Ops) lets employees know that management is prioritizing these functions. This in turn leads to IT Ops and Sec Ops teams being provided the appropriate resources required to fulfill their missions.

- **Do all users receive appropriate education about IT Ops and SecOps functions and missions?** Security awareness training for DIB personnel is nothing new but having it be its own security domain within NIST/CMMC continues to enforce its importance. Users need to be aware of the role they play in ensuring their IT environment stays reliable and secure. Educating users about security awareness needs not only be a once a year exercise. Content and best practices should be communicated continuously to promote a culture of security and risk awareness. And just as we expect a minimum level of education for our general user base, those in charge of managing our IT systems need to also consider what specialized education and training is needed to stay ahead of emerging threats and technologies.

- **Do you have the right resources in place?** While this certainly includes having the right technology to support your organization's security posture, it also includes having the right human resources. Having individuals with appropriate knowledge of both IT Ops and Sec Ops will be helpful to work effectively with those who may only have experience in only one of those areas. Looking solely through a security lens may potentially cause blind spots when looking at the bigger picture. If implementing a security fix causes an application to become near unusable, was the cost/benefit properly analyzed? This is increasingly important as technology and systems become increasingly complex due to outsourcing, and use of cloud platforms, and other reasons.

Having a strong Sec Ops functions in place is critical to ensuring that your organizational stays secure and compliant. However, there are also complementary functions needed to implement required security practices. It is a balancing act to ensure organizational and business needs while addressing security and regulatory requirements. Having the right system knowledge, understanding of supporting functions, support, and resources, will be essential to achieving and maintaining compliance with CMMC practices at your desired maturity level.

About Aronson LLC

Aronson LLC provides a comprehensive platform of assurance, tax, and consulting solutions to today's most active industry sectors and successful individuals. As a nationally ranked public accounting firm, with a dedicated government consulting practice and technology advisory focus, Aronson offers a unique value proposition to government contractors. Aronson has a pending application with the CMMC Accreditation Board (CMMC-AB) to become a Registered Provider Organization (RPO). For more information about Aronson LLC, please visit www.aronsonllc.com or call 240.630.0702.

AZUNNA ANYANWU
Director of Information Technology
aanyanwu@aronsonllc.com
301.231.6235