2021

Why is CMMI Level 3 Relevant for Cybersecurity?

(202) 996-9166 | info@mmgllc.us | www.mmgllc.us

MAGNUS
Management Group LLC
Build - Manage - Protect

Background

Maturity models have been around for more than three decades, as early as the 1980s. The original intent of the Capability Maturity Model (CMM) was to assess the United States Department of Defense (D.O.D.) contractors' processes. The success of the software projects was measured using the CMM measurements. Higher maturity scores were equivalent to better processes. Higher scores also meant that the contractors used established and reputable processes and best practices for software design, development and quality assurance.

The context in which the term 'maturity' was used had special significance. It was used in reference to specific aspects of the assessment, where the level of organization and optimization of each operation could range from ad hoc to formal. Because CMM's initial focus was particularly aimed at improving the software development process, its scope and application was very limited. For this reason, the Software Engineering Institute (SEI) at Carnegie Mellon University revised it. It then became known as the Capability Maturity Model Integration (CMMI). This new framework superseded the original CMM in scope.

The extended scope of CMMI now allows it to have a footprint in multiple disciplines. These include Information and Communication Technology (ICT), business process management, service management, civil engineering, manufacturing and cybersecurity.

What is CMMI?

The Capability Maturity Model Integration (CMMI) is a framework that improves processes. It is also considered a measurement tool where an enterprise can benefit from its operation's effectiveness being measured to identify how improvements can be achieved over time.

Once the brainchild of the U.S. D.O.D., CMMI is now administered by the CMMI Institute. The institute itself was purchased in 2016 by the Information Systems and Control Association (ISACA). With CMMI now being housed by an international organization, it currently serves entities globally both in ICT service management and software engineering.

The main target enterprises for CMMI are those that supply government products or services. These entities are often asked to meet the minimum CMMI level 3 across their core delivery operations. There are five maturity levels in total with one being the least ideal state while 5 is the most ideal state of maturity. At level five an entity's operations are fully optimized across the business and managed under a continuous process improvement system. While it is the coveted state for organizations to be, level 3 is most attainable for organizations. It is also sufficient since it shows a level of maturity that requires the use of formal methods of design, development, testing and delivery.

There are five maturity levels in the CMMI framework. They follow the original guideline of CMM. The five levels are:

1. **Initial** - The documentation process is localized and formal. General business procedures however, are somewhat ad hoc and undefined.
2. **Managed** - There is an agreed metrics that determines how processes are managed, but, there is nothing in place to assess its success or gather feedback. In essence, procedures are followed but there is no way to measure its efficacy nor is there any consistency in following a set procedure.
3. **Defined** - Standard business procedures are structured and thoroughly outlined. Operations are broken down into detailed processes, work instructions and artifacts that are used to record process outputs.
4. **Quantitatively Managed** - Process governance committee is employed to gather measurements from each operation. This information is then analyzed, and a success report is issued.
5. **Optimizing** - An established process management system is in place. It focuses on process improvement and disciplined optimization. A team of business analysts are employed to measure and assess the entire business operation for gaps and possible opportunities for improvement.

Ideally companies should strive to attain level five, however this may not always be practical because of the effort and resources that are involved. It is for this reason organizations are encouraged to attain level 3. While maturity level 3 is not the optimized state, it does provide the level of confidence that the organization is striving to optimize its business processes.

Crosswalk between CMMI to CMMC

The purpose of this white paper is to explain why CMMI level 3 is relevant for Cybersecurity. To achieve this a crosswalk between CMMI and CMMC must be established. To begin with, we need to first understand the relationship between the two. The U.S. Department of Defense has taken a keen interest in process maturity, so it's no surprise they have released their own approach to cybersecurity maturity in the Cybersecurity Maturity Model Certification (CMMC) Framework.

Like CMMI, CMMC also has five levels of certification that measures the maturity of cyber processes. Identical to CMMI, the levels run from Initial through to Optimized, except that CMMC levels are specific to cybersecurity. The five levels rank progressively with the next succeeding tier developing from the previous one with specific technical requirements. Its processes are broken down into 17 distinct security domains that are akin to the NIST Cyber security Framework

(CSF). As such, CMMC can be used alongside the CSF to design, build, deliver and operate an optimized and continually progressive security program.

The CMMC levels are defined as follows:

1. **Level 1**: Basic cyber hygiene practices are to be performed. This includes ensuring that employees regularly change their passwords and software antivirus is used.
2. **Level 2**: Intermediary cyber hygiene practices should be documented, practiced and used in the process of protecting Controlled Unclassified Information (CUI) through the implementation of NIST 800-171 revised (r)1 security requirements.
3. **Level 3**: Good cyber hygiene practices are implemented using institutionalized management procedures. The process is used to safeguard CUI, this includes all the NIST 800-171 r1 security requirements and any other related standards.
4. **Level 4**: Processes for evaluating and measuring the effectiveness of practices that detect and respond to changing strategies, methods, and procedures of Advanced Persistent Threats (APT) are implemented. Additional enhanced practices are also performed to detect APTs' tactics.
5. **Level 5**: The best and most reputable standards are implemented and optimized to provide the most sophisticated capabilities to detect and respond to APTs. Additional enhanced practices are also performed to detect APTs' methods and counter their tactics.

As shown from the CMMC model, the continuum follows a similar blueprint as the CMMI model. In fact, both models draw from the same domain source and are almost identical in some respects. The only difference with CMMC is that it is specifically tailored for cybersecurity.

To complete the crosswalk between CMMI and CMMC we will examine the similarities they share at each level:

- **Level 5: Nearly exact matches are:**
    - Configuration management
    - Risk management
    - Incident Response
        - Incident Response and Prevention, Causal Analysis Resolution, Verification and Validation
- **Level 4: Very Close Match**
    - Audit and Accountability
        - Process Quality Assurance

        - Configuration Management
    - Recovery
    - Awareness and Training (Organizational Training)
- **Level 3: Partial Match**
    - Media Protection (Configuration Management)
    - Identification and Authentication (Configuration Management)
    - Access Control (Configuration Management, Monitor and Control)
    - Asset Management
        - Configuration Management
        - Monitor and Control
        - Process Asset Development

There is very little resemblance at levels 2 and 1 with level 2 showing a vague match and level one showing no match at all.

CMMI Version 2 - Security and Safety

The introduction of CMMI v2 has shown that the maturity model has moved away from the general capability models and taken on a more cybersecurity flavor. ISACA's new CMMI Model details all the best practices for thoroughly defining security and safety methods, approaches, actions and tasks necessary to safeguard an enterprise's entire ecosystem, including data, personnel and resources.

This version has new content, namely: Capability Area (CA) and Managed Security and Safety (MSS). CA is about the evaluation and identification of safety and security constraints and needs. It also includes planning and prioritizing the best approaches to tackle those needs and constraints. Most importantly, it involves responding to and preventing harmful events and incidents and protecting and defending against safety incidents and security threats and vulnerabilities.

MSS on the other hand describes the capability organizations need to:

- **Prepare:** Define the appropriate approach for organizational readiness and preparedness to tackle safety security requirements and limitations.
- **Investigate:** Examine, research, and learn from past security incidents and experiences
- **Monitor:** Discover and counter any event or incidents that can cause harm to the enterprise. Additionally, to find solutions to potential events on a consistent basis.
- **Protect and Defend:** Implement preventative measures against present and future potentially harmful events on the enterprise. To execute measures that will either avoid or minimize harmful threats on the entity.

- **Preempt and Prevent:** Perform advanced security analysis to forecast and avoid threats, vulnerabilities, schemes, activities caused by personnel, systems or processes (both internal and external) that may be harmful to the enterprise.
- **Review and Evaluate:** Discern the effectiveness of safety and security measures implemented and make improvements.

Since Cybersecurity practices have become a central part of an enterprise's maturity, CMMI V2 now guides companies towards that end (Cybersecurity Maturity). For example, managing Security Threat and Vulnerability is a central theme in cybersecurity and is now one of the new practice areas of CMMI. It includes a holistic and systematic approach for addressing security threats and vulnerabilities for an organization, project or work effort to select which threats and vulnerabilities are the most critical to tackle, given the possible risk and impact to the enterprise's mission.

Why is CMMI Level 3 Relevant for Cybersecurity?

As alluded to earlier, CMMI Level 3 is one of the five maturity levels in the CMMI. of significance, most companies working with CMMI today are at this maturity level. Known as the "Defined" level, it is achieved when an enterprise successfully completes a SCAMPI A appraisal (Standard CMMI Appraisal Method for Process Improvement). Attaining this level says three things about your company:

1. Your processes and quality are at par with the globally accepted standards and nomenclatures
2. You are more proactive than reactive in tackling risks and
3. You have operated abiding by the process guideline that gives guidance for your procedures.

Another significance of attaining CMMI Level 3 is showing that your organization is cybersecurity compliant. Earlier in this paper the comparison was made with CMMC. It was established that both share close relations. CMMI Level 3 in particular, though not as identical as levels 4 and 5, shares similarities with its CMMC equivalent in three areas, namely: Media Protection, Access Control, Identification and Authentication. Of notable interest, all three areas are from the NIST 800-53 Control Families.

Media Protection

Media Protection is primarily focused on the security of media storage. This includes who can access the stored content, how transportation is controlled, and the safe use of storage devices. Some of the key points addressed in this family are:

- **Securely store paper and digital content** - Both digital media content and printed material are to be securely kept in restricted and protected areas. Examples of such secured areas include a cabinet that requires a physical lock (this in the case of printed material) or a secure server (in the case of digital media).
- **Restrict access to protected information to authorized users** - Only authorized users should be allowed access to company systems. As it relates to access to physical storage areas, coded keypads, key cards, keys or other forms of locks should be installed to restrict the free movement in and out of these areas. Concerning digital storage areas, two-factor authentication should be enforced.
- **The sharing and transporting of protected data should be managed** - Content deemed as secure should be protected, as such, only authorized devices and personnel should be allowed to transport protected data. The media that once stored protected data must be properly destroyed to avoid accidental data leakage.
- **Strict restrictions should be enforced on the use of portable devices** - Only known and identifiable authorized users should be allowed to use portable devices to access company systems.

Access Control

Access Control addresses the matter of authorized access to entity controls. Access should be restricted to only trusted users and devices. Access control deals with the following matters:

- **Restrict system access to authorized users** - To begin with, authorized users usually belong to the entity as employee or contractor. They are assigned roles, groups and accounts. Any user outside of an assigned account login credential is not allowed to access the system.
- **Access is tailored to job roles and duties** - System roles and permissions should be assigned based on the job requirement of the employee. For example, only financial personnel should be able to access budget workbooks and therefore access to these files would be denied for other job roles.
- **Restrict access to admin functions** - Assign edit or modify permissions only to those authorized users who make the changes. As it relates to view permissions, this may be shared with others as the need arises.
- **Control remote access to your systems** - Establish requirements and restrictions for remote access including the levels of access that are permitted to authorized users while they are using remote access.
- **Control wireless and mobile device access to your systems** - Establish wireless and mobile device guidelines and restrictions. Ensure using verification methods that only trusted devices are operated by authorized users.

MAGNUS
Management Group LLC
Build - Manage - Protect

Identification and Authentication

The focus of this family is verifying that the people who are accessing your systems are the ones authorized to do so. Some of the main points are as follows:

- **Before any personnel or device can access your system, they should be identified and verified** - The login information for the user and the device that is being used to access your system must match the authorized list and can be traced to an assigned and approved user.
- **A minimum complexity for passwords should be enforced** - Authorized users should be aided in their efforts to keep their passwords secure. This can be done by giving them clear direction in the form of a password policy. Your password protocols will establish the complexity of their passwords, for example: the length of the password, the inclusion of numerals, uppercase letters, or whether special characters are required.
- **Multifactor authentication for network access must be established** - In addition to the conventional authentication methods (User ID and Password), ensure at the very least two-factor authentication. This may require another authentication tool which may be in the form of a numeric code that is sent to a user's mobile device or a fingerprint scanner.
- **Implement an access time-out feature to disable access after a period of account inactivity** - a session time-out program should be utilized where network connectivity will be terminated after a specified time. This will protect data from unauthorized exposure when not in use or the user has wandered away from a system leaving it idle.

Conclusion

In response to the question of "why is CMMI Level 3 relevant for Cybersecurity", we looked first at the relationship between the two entities (i.e. CMMI and Cybersecurity), then examined the depth of the relationship. At the start, DOD in collaboration with Carnegie Mellon University developed CMMI as a maturity framework to assess the level of organization and optimization of an enterprise's processes. The industries ranged from manufacturing to technology and importantly cybersecurity. With CMMI's focus divided among several industries, the DOD created the CMMC focused on Cybersecurity. From its inception it was clear that CMMC draws its inspiration from CMMI as both maturity models share a similar framework, even drawing from the same pool of the NIST 800-53 controls. ISACA, (the current owners of the CMMI) have upgraded the model to version 2 moving away from the general capability models for a more cybersecurity centric model. This making CMMI 2.0 more cybersecurity focused and in line with DOD requirements. It will be interesting to see how CMMC AB will look to CMMI 2.0 since at the time of publishing of this article, CMMC standards have not been finalized.