CMM #	CMMC v1.02	CMMC v1.2 - Definition	SP-CMM	SP-CMM - Definition	COBIT 4	COBIT 4 - Definition	ISO 15504	ISO 15504 (COBIT 5) - Definition	CMMI	CMMI - Definition
0	N/A	N/A	Not Performed	There is general failure to attain the purpose of the process.	Non-Existent	There is no recognition of the need for internal control. Control is not part of the organization's culture or mission. There is a high risk of control deficiencies and incidents.	Incomplete	There is general failure to attain the purpose of the process. There are few or no easily identifiable work products or outputs of the process.	Incomplete	Incomplete approach to meeting the intent of the Practice Area. - Inconsistent performance. - Ad hoc and unknown. - Work may or may not get completed.
1	Performed	Mission: Safeguard Federal Contract Information (FCI) **Processes: Performed** Level 1 requires that an organization performs the specified practices. Because the organization may only be able to perform these practices in an ad-hoc manner and may or may not rely on documentation, process maturity is not assessed for Level 1. **Practices: Basic Cyber Hygiene** Level 1 focuses on the protection of FCI and consists only of practices that correspond to the basic safeguarding requirements specified in 48 CFR 52.204-21 ("Basic Safeguarding of Covered Contractor Information Systems").	Performed Informally	Base practices of the process area are generally performed. The performance of these base practices may not be rigorously planned and tracked. Performance depends on individual knowledge and effort. Work products of the process area testify to their performance. Individuals within the organization recognize that an action should be performed, and there is general agreement that this action is performed as and when required. There are identifiable work products for the process.	Initial & Ad-Hoc	There is some recognition of the need for internal control. The approach to risk and control requirements is ad hoc and disorganized, without communication or monitoring. Deficiencies are not identified. Employees are not aware of their responsibilities.	Performed	Individuals within the organization recognize that an action should be performed, and there is general agreement that this action is performed as and when required. There are identifiable work products for processes and these testify to the achievement of the purpose. The purpose of the process is generally achieved. The achievement may not be rigorously planned and tracked.	Initial	At maturity level 1, processes are usually ad hoc and chaotic. The organization usually does not provide a stable environment. Success in these organizations depends on the competence and heroics of the people in the organization and not on the use of proven processes. Maturity level 1 organizations often produce products and services that work; however, they frequently exceed the budget and schedule of their projects. Maturity level 1 organizations are characterized by: - A tendency to over commit, abandon processes in the time of crisis, and not be able to repeat their past successes. - Not a complete set of practices to meeting the full intent of the Practice Area.
2	Documented	Mission: Serve as a transition step in cybersecurity maturity progression to protect CUI **Processes: Documented** Level 2 requires that an organization establish and document practices and policies to guide the implementation of their CMMC efforts. The documentation of practices enables individuals to perform them in a repeatable manner. Organizations develop mature capabilities by documenting their processes and then practicing them as documented. **Practices: Intermediate Cyber Hygiene** Level 2 serves as a progression from Level 1 to Level 3 and consists of a subset of the security requirements specified in NIST SP 800-171 as well as practices from other standards and references. Because this level represents a transitional stage, a subset of the practices reference the protection of CUI.	Planned & Tracked	Performance of the base practices in the process area is planned and tracked. Performance according to specified procedures is verified. Work products conform to specified standards and requirements. Measurement is used to track process area performance, thus enabling the organization to manage its activities based on actual performance. The primary distinction from Level 1, Performed Informally, is that the performance of the process is planned and managed.	Repeatable but Intuitive	Controls are in place but are not documented. Their operation is dependent on knowledge and motivation of individuals. Effectiveness is not adequately evaluated. Many control weaknesses exist and are not adequately addressed; the impact can be severe. Management actions to resolve control issues are not prioritized or consistent. Employees may not be aware of their responsibilities.	Managed	Work products conform to specified standards and requirements. The process delivers work products according to specified procedures and is planned and tracked. The primary distinction from the Performed Level (CMM1) is that the performance of the process now delivers work products that fulfil expressed quality requirements within defined timescales and resource needs.	Managed	At maturity level 2, work groups establish the foundation for an organization to become an effective organization by institutionalizing selected Project and Work Management, Support, and Service Establishment and Delivery processes. Work groups define a service strategy, create work plans, and monitor and control the work to ensure the service is delivered as planned. The organization establishes agreements with customers and develops and manages customer and contractual requirements. Configuration management and process and product quality assurance are institutionalized, and the organization also develops the capability to measure and analyze process performance. Also at maturity level 2, work groups, work activities, processes, work products, and services are managed. The organization ensures that processes are planned in accordance with policy. To execute the process, the organization provides adequate resources, assigns responsibility for performing the process, trains people on the process, and ensures the designated work products of the process are under appropriate levels of configuration management. The organization identifies and involves relevant stakeholders and periodically monitors and controls the process.
3	Managed	Mission: Protect Controlled Unclassified Information (CUI) **Processes: Managed** Level 3 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. **Practices: Good Cyber Hygiene** Level 3 focuses on the protection of CUI and encompasses all of the security requirementsspecified in NIST SP 800-171 as well as additional practices from other standards andreferences to mitigate threats. It is noted that DFARS clause 252.204-7012 ("Safeguarding of Covered Defense Information and Cyber Incident Reporting") specifies additional requirements beyond the NIST SP 800-171 security requirements such as incident reporting.	Well Defined	Base practices are performed according to a well-defined process using approved, tailored versions of standard, documented processes. The primary distinction from Level 2, Planned and Tracked, is that the process is planned and managed using an organization-wide standard process.	Defined Process	Controls are in place and are adequately documented. Operating effectiveness is evaluated on a periodic basis and there is an average number of issues. However, the evaluation process is not documented. Whilst management is able to deal predictable with most control issues, some control weaknesses persist and impacts could still be severe. Employees are aware of their responsibilities for control.	Established	The process is performed and managed using a defined process based upon good engineering principles. The resources necessary to establish the process definition are also in place. The primary distinction from the Managed Level (CMM2) is that the process of the Established Level is using a defined process that is capable of achieving its process outcomes.	Defined	At maturity level 3, organizations use defined processes for managing work. They embed tenets of project and work management and services best practices, such as service continuity and incident resolution and prevention, into the standard process set. The organization verifies that selected work products meet their requirements and validates services to ensure they meet the needs of the customer and end user. These processes are well characterized and understood and are described in standards, procedures, tools, and methods. The organization's set of standard processes, which is the basis for maturity level 3, is established and improved over time. These standard processes are used to establish consistency across the organization. Work groups establish their defined processes by tailoring the organization's set of standard processes according to tailoring guidelines. At maturity level 3, processes are managed more proactively using an understanding of the interrelationships of process activities and detailed measures of the process, its work products, and its services. At maturity level 3, the organization further improves its processes that are related to the maturity level 2 process areas.
4	Reviewed	Mission: Protect CUI and reduce the risk of Advanced Persistent Threats (APTs) **Processes: Reviewed** Level 4 requires that an organization review and measure practices for effectiveness. In addition to measuring practices for effectiveness, organizations at this level are able to take corrective action when necessary and inform higher level management of status or issues on a recurring basis. **Practices: Proactive** Level 4 focuses on the protection of CUI from APTs and encompasses a subset of the enhanced security requirements from Draft NIST SP 800-171B as well as other cybersecurity best practices. These practices enhance the detection and response capabilities of an organization to address and adapt to the changing tactics, techniques, and procedures (TTPs) used by APTs.	Quantifatively Controlled	Detailed measures of performance are collected and analyzed. This leads to a quantitative understanding of process capability and an improved ability to predict performance. Performance is objectively managed, and the quality of work products is quantitatively known. The primary distinction from the Well Defined level is that the defined process is quantitatively understood and controlled.	Managed & Measurable	There is an effective internal control and risk management environment. A formal, documented evaluation of controls occurs frequently. Many controls are automated and regularly reviewed. Management is likely to detect most control issues, but not all issues are routinely identified. There is consistent follow-up to address identified control weaknesses. A limited, tactical use of technology is applied to automated controls.	Predictable	Detailed measures of performance are collected and analyzed. This leads to a quantitative understanding of process capability and an improved ability to predict and manage performance. Performance is quantitatively managed. The primary distinction from the Established Level (CMM3) is that the defined process is now performed consistently within defined limits to achieve its process outcomes.	Quantitatively Managed	At maturity level 4, organizations establish quantitative objectives for quality and process performance and use them as criteria in managing processes. Quantitative objectives are based on the needs of the customer, end users, organization, and process implementers. Quality and process performance is understood in statistical terms and is managed throughout the life of processes. Process performance baselines and models can be used to set quality and process performance objectives that help achieve business objectives. A critical distinction between maturity levels 3 and 4 is the predictability of process performance. At maturity level 4, the performance of processes is controlled using statistical and other quantitative techniques and predictions are based, in part, on a statistical analysis of fine-grained process data.
5	Optimizing	Mission: Protect CUI and reduce the risk of Advanced Persistent Threats (APTs) **Processes: Optimizing** Level 5 requires an organization to standardize and optimize process implementation across the organization. **Practices: Advanced/Proactive** Level 5 focuses on the protection of CUI from APTs. The additional practices increase the depth and sophistication of cybersecurity capabilities.	Continuously Improving	Quantitative performance goals (targets) for process effectiveness and efficiency are established, based on the business goals of the organization. Continuous process improvement against these goals is enabled by quantitative feedback from performing the defined processes and from piloting innovative ideas and technologies. The primary distinction from the quantitatively controlled level is that the defined process and the standard process undergo continuous refinement and improvement, based on a quantitative understanding of the impact of changes to these processes.	Optimized	An enterprise risk and control program provides continuous and effective control and risk issues resolution. Internal control and risk management are integrated with enterprise practices, supported with automated real-time monitoring with full accountability for control monitoring, risk management and compliance enforcement. Control evaluation is continuous, based on self-assessments and gap and root cause analysis. Employees are proactively involved in control improvements.	Optimizing	Optimizing a process involves piloting innovative ideas and technologies and changing non-effective processes to meet defined goals or objectives. The primary distinction from the Predictable Level (CMM4) is that the defined and standard processes now dynamically change and adapt to effectively meet current and future business goals.	Optimizing	At maturity level 5, an organization continually improves its processes based on a quantitative understanding of its business objectives and performance needs. The organization uses a quantitative approach to understand the variation inherent in the process and the causes of process outcomes. Maturity level 5 focuses on continually improving process performance through incremental and innovative process and technological improvements. The organization's quality and process performance objectives are established, continually revised to reflect changing business objectives and organizational performance, and used as criteria in managing process improvement. A critical distinction between maturity levels 4 and 5 is the focus on managing and improving organizational performance. At maturity level 4, the organization and work groups focus on understanding and controlling performance at the subprocess level and using the results to manage projects. At maturity level 5, the organization is concerned with overall organizational performance using data collected from multiple work groups. Analysis of the data identifies shortfalls or gaps in performance. These gaps are used to drive organizational process improvement that generates measureable improvement in performance.