CMMI V2.0 and the CyberSecurity Maturity Model Certification (CMMC): a Crosswalk

CAPABILITY COUNTS 2020

Margaret Tanner Glover,
CMMI High Maturity Lead Appraiser, Scaled Agile Program Consultant
Certified Cloud Security Consultant, ISO 27001 Lead Auditor for Information Security

CMMI® Institute
AN ISACA ENTERPRISE

Today's Topics

Goal: Leveraging your CMMI expertise to support CMMC

1. Quick CMMC overview
2. CMMI and CMMC similarities: Domains, Practice Areas, Capability Levels
3. CMMI-CMMC direct overlap (Risk Management)
4. CMMI-CMMC little to no overlap (Physical Protection)
5. Other resources such as (ISO 27001,) NIST 800-171, CERT RMM, etc.

All your organization's hard work for continued CMMI compliance pays off for CMMC!

CMMC Overview

CMMC: What Who When How

What: It is a *certification*: Cybersecurity Maturity Model Certification *to a model*

Who: Currently applies to anyone who does business with the Department of Defense; likely will expand to other areas of federal government

When: Being solidified; larger organizations will probably begin Sept 2020

How: Appraisal providers, method to document, cost, etc. not yet defined

CMMC: Background

Applies to:

1. Existing DoD contracts throughout **supply chain**
2. Ability to provide RFPs including **team** members and **subcontractors**

The CMMC'S role is to safeguard FCI requirements specified in the FAR Clause 52.204-21 and the security requirements for CUI in the NIST SP 800-171 per the DARS Clause 252.204-7012 (3,4,5).

CMMC Goal: stop the information leakage at all levels

CMMC: What you need to know

The CMMC adds a **certification element** to verify the implementation of process and practices associated with the achievement of a cybersecurity maturity level. These Maturity Levels provide increased assurance to the DoD that a DIB contractor can protect CUI at a level the risk, accounting for information flow down to the subcontractors in a multi –tier supply chain.

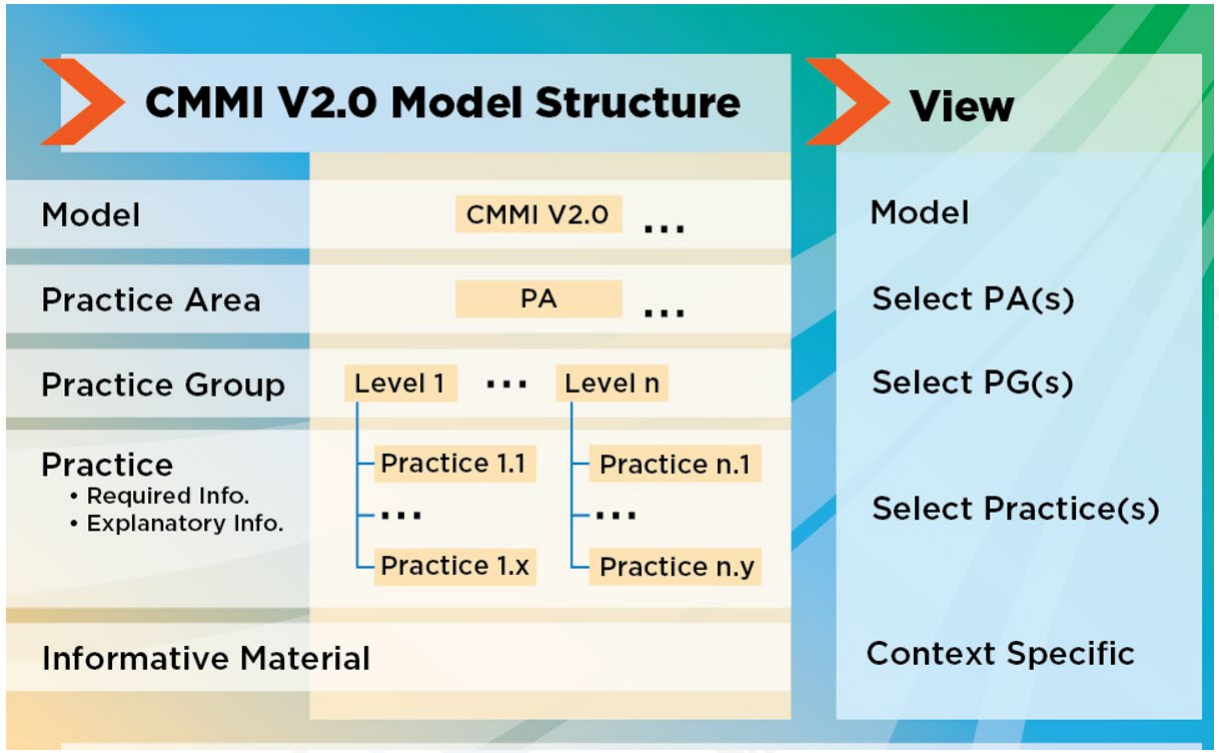
CMMC is a DoD certification process that measures a DIB sector company's ability to protect FCI and CUI, much in the same way the CMMI measures the performance through building and benchmarking key capabilities to align to business goals for process improvement.

The CMMC has been developed by the Software Engineering Institute and the John's Hopkins University Applied Physics Laboratory

Comparing CMMI V2 Frameworks and Taxonomy to CMMC

CMMI V2 structure

Figure 8. CMMI Model Structure



CMMC Hierarchy

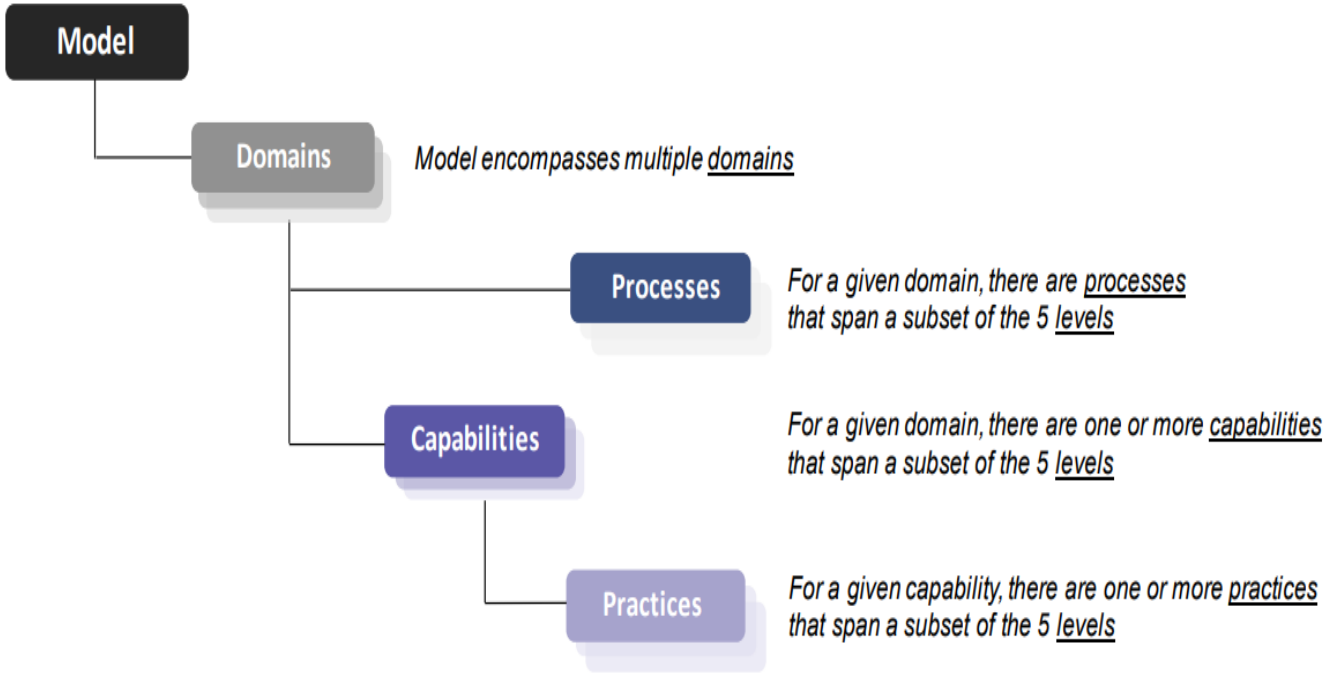


Figure 1. CMMC Model Framework (Simplified Hierarchical View)

CMMC Levels

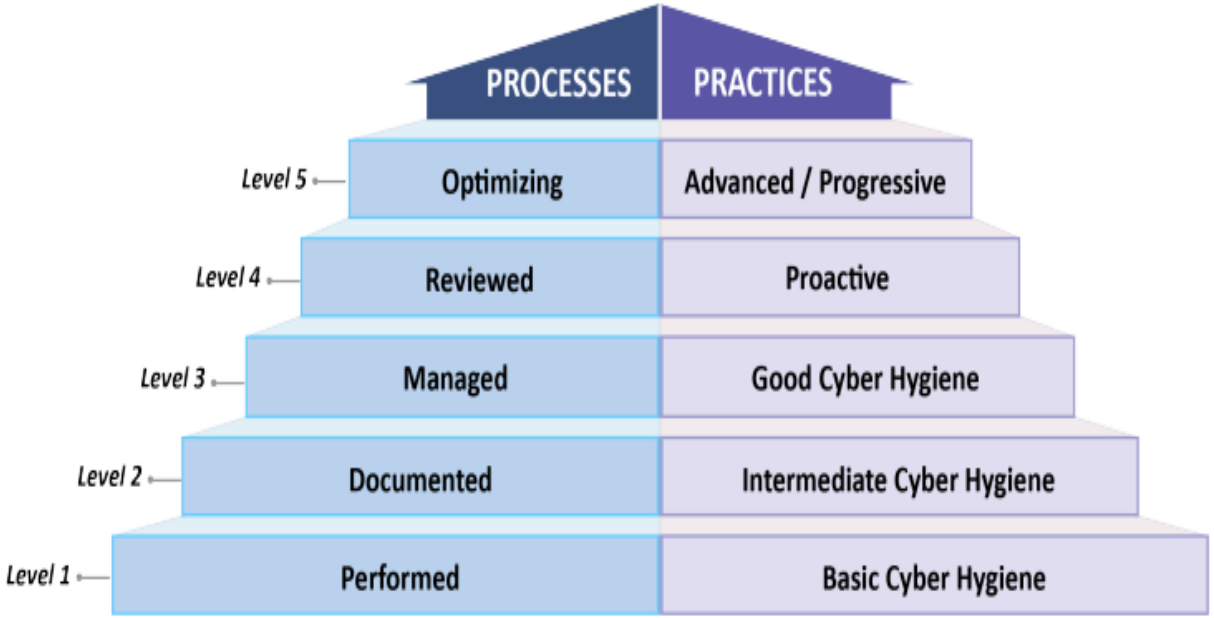
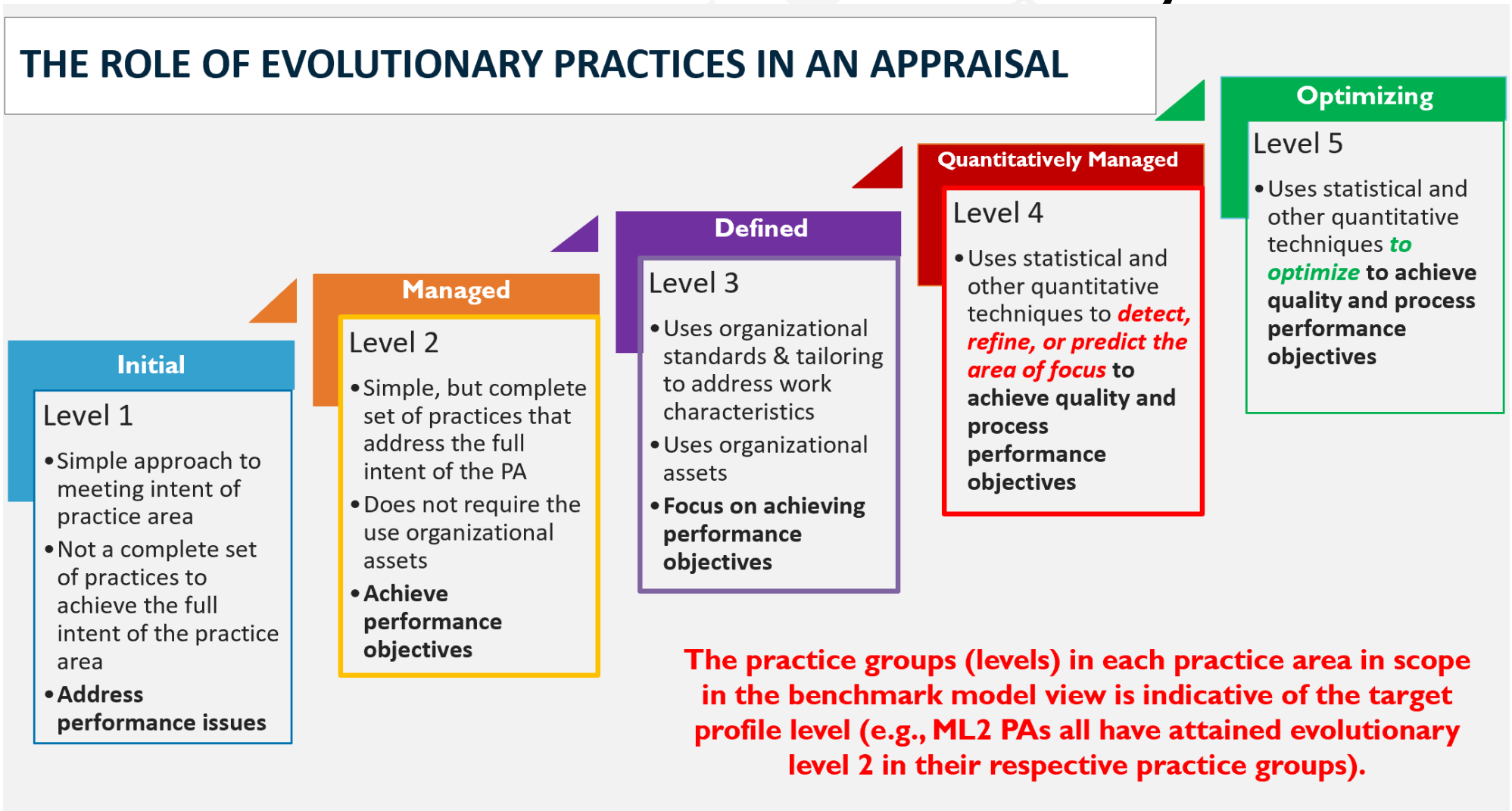


Figure 2. CMMC Levels and Descriptions

Just as in CMMI V2, the levels are cumulative. For example, to achieve Level 3, you must demonstrate achievement of all the lower levels (Level 1 and Level 2).

CMMI Process Maturity



Summary of CMMC Maturity Levels

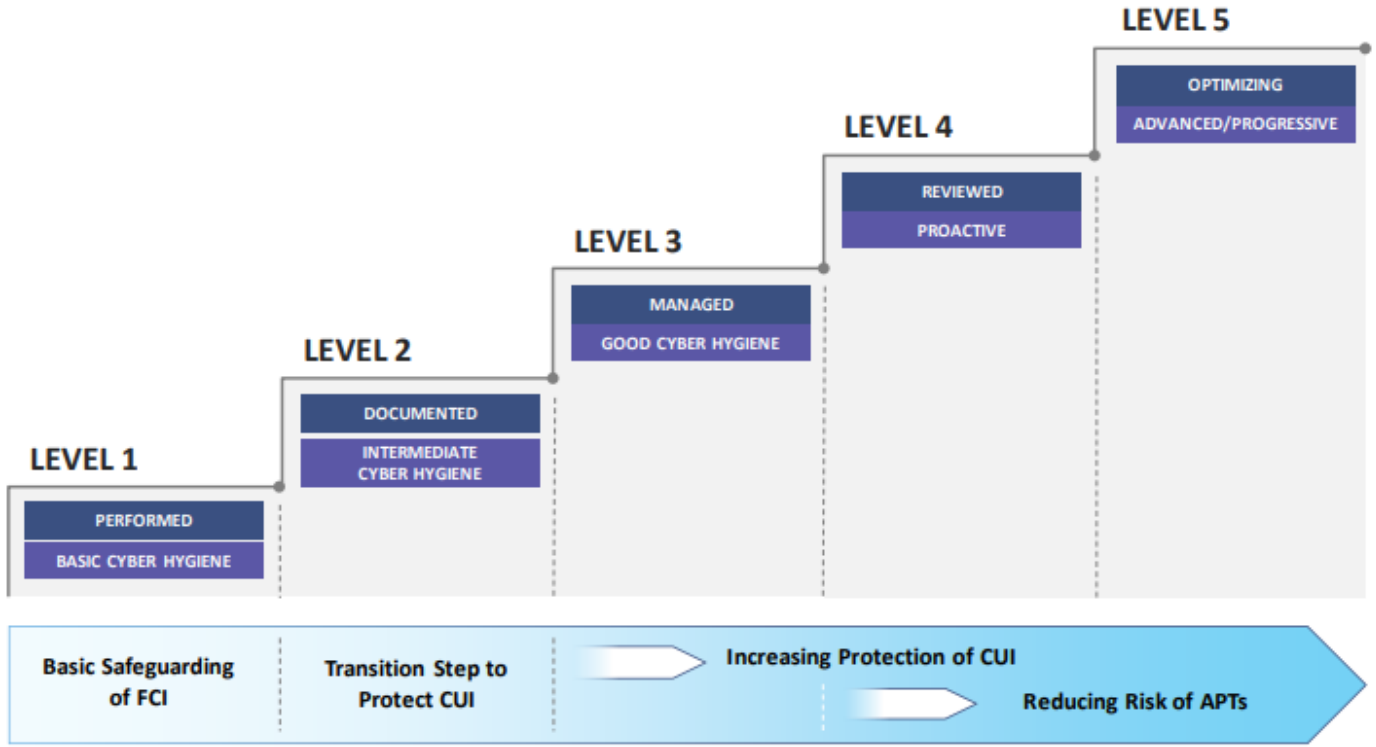


Figure 3. CMMC Levels and Associated Focus

CMMI Practice Areas

CMMC Domains

Figure 4. CMMC Domains

CMMC Domains

and Capabilities

Table 1. CMMC Capabilities

Domain	Capability
Access Control (AC)	• Establish system access requirements • Control internal system access • Control remote system access • Limit data access to authorized users and processes
Asset Management (AM)	• Identify and document assets
Audit and Accountability (AU)	• Define audit requirements • Perform auditing • Identify and protect audit information • Review and manage audit logs
Awareness and Training (AT)	• Conduct security awareness activities • Conduct training
Configuration Management (CM)	• Establish configuration baselines • Perform configuration and change management
Identification and Authentication (IA)	• Grant access to authenticated entities
Incident Response (IR)	• Plan incident response • Detect and report events • Develop and implement a response to a declared incident • Perform post incident reviews • Test incident response
Maintenance (MA)	• Manage maintenance
Media Protection (MP)	• Identify and mark media • Protect and control media • Sanitize media • Protect media during transport
Personnel Security (PS)	• Screen personnel • Protect CUI during personnel actions
Physical Protection (PE)	• Limit physical access
Recovery (RE)	• Manage back-ups
Risk Management (RM)	• Identify and evaluate risk • Manage risk
Security Assessment (CA)	• Develop and manage a system security plan • Define and manage controls • Perform code reviews
Situational Awareness (SA)	• Implement threat monitoring
Systems and Communications Protection (SC)	• Define security requirements for systems and communications • Control communications at system boundaries
System and Information Integrity (SI)	• Identify and manage information system flaws • Identify malicious content • Perform network and system monitoring • Implement advanced email protections

CMMC Processes and Institutionalization

Table 2. CMMC Processes

Maturity Level	Maturity Level Description	Processes
ML 1	**Performed**	*There are no maturity processes assessed at Maturity Level 1.* *An organization performs Level 1 practices but does not have process institutionalization requirements.*
ML 2	**Documented**	Establish a policy that includes [DOMAIN NAME].
		Document the CMMC practices to implement the [DOMAIN NAME] policy.
ML 3	**Managed**	Establish, maintain, and resource a plan that includes [DOMAIN NAME].
ML 4	**Reviewed**	Review and measure [DOMAIN NAME] activities for effectiveness.
ML 5	**Optimizing**	Standardize and optimize a documented approach for [DOMAIN NAME] across all applicable organization units.

The CMMC maturity levels serve as a way to measure an organization's process maturity or process institutionalization. This characterizes the extent to which an activity is embedded or ingrained in operations of an organization. Just like II and GOV in CMMI V2.

CMMI V2 and CMMC

Correlations between Domains and Practice areas:

Reuse and Extend

Crosswalk of CMMI V2 to CMMC

5: Nearly Exact Matches are:

- Configuration Management
- Risk Management
- Incident Response (Service View: Incident Response and Prevention, Causal Analysis and Resolution, Dev View: Verification and Validation)

Domains from CMMC vs. **Practice Areas** in CMMI V2 matches:

5=Nearly Exact **4**=Very Close **3**=Partial **2**=Vague **1**=No Match

CMMI PA	CMMC Domain
Incident Resolution and Prevention (IRP)	Incident Resolution (IR)
Continuity (CONT)	Situational Awareness (SA)
Risk and Opportunity Management (RSK)	Risk Management (RM)

CMMI V2 Risk and Opportunity Management

Risk: a potential uncertain event that may be harmful or may negatively impact be achieving objectives (from the CMMI V2 glossary).

Risk and Opportunity Management Practice Area

- Intent: **Identify**, **record**, **analyze** and **manage** potential risks or opportunities
- Value: **Mitigate** adverse impacts or **capitalize** on positive impacts to increase the likelihood of meeting objectives.

RSK is at L1, L2 and L3.

Practice Summary

LEVEL 1	RSK 1.1	Identify and record risks or opportunities and keep them updated.
LEVEL 2	RSK 2.1	Analyze identified risks or opportunities.
	RSK 2.2	Monitor identified risks or opportunities and communicate status to affected stakeholders.
LEVEL 3	RSK 3.1	Identify and use risk or opportunity categories.
	RSK 3.2	Define and use parameters for risk or opportunity analysis and handling.
	RSK 3.3	Develop and keep updated a risk or opportunity management strategy.
	RSK 3.4	Develop and keep updated risk or opportunity management plans.
	RSK 3.5	Manage risks or opportunities by implementing planned risk or opportunity management activities.

CMMC Risk Management

CMMC Capability 031: Identify and Evaluate Risk

Level 2: P1141:

Periodically **assess the risk** to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of Federal Contract Information.

- NIST SP 800-171 3.11.1:
- CERT RMM v1.2 RISK: SG4:

CMMI RSK 2.1 **Analyze identified risks** or opportunities

CMMC Risk Management

CMMC Capability 031: Identify and Evaluate Risk
Level 3: Practice 1144

Periodically Perform risk assessments to i**dentify** and prioritize risks according to the defined **risk categories**, risk sources, and risk measurement criteria

- NIST CSF v1.1 RA
- CERT RMM v1.2 RISK: SG3 and SG4.SP3

CMMI RSK 3.1 I**dentify** and use **risk** or opportunity **categories**

DOMAIN: RISK MANAGEMENT (RM)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C031 Identify and evaluate risk		P1141 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of Federal Contract Information. • NIST SP 800-171 3.11.1 • CERT RMM v1.2 RISK:SG4	P1144 Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources, and risk measurement criteria. • NIST CSF v1.1 ID.RA • CERT RMM v1.2 RISK:SG3 and SG4.SP3	P1149 Catalog and periodically update threat profiles and adversary TTPs. • NIST CSF v1.1 DE.AE-2	
		P1142 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. • NIST SP 800-171 3.11.2		P1150 Employ threat intelligence to inform the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, and response and recovery activities. • NIST SP 800-171B 3.11.1e • NIST CSF v1.1 ID.RA-2 and ID.RA-3	
				P1151 Perform scans for unauthorized ports available across perimeter network boundaries over the organization's Internet network boundaries and other organizational-defined boundaries. • CIS Controls v7.1 12.2	
C032 Manage risk		P1143 Remediate vulnerabilities in accordance with risk assessments. • NIST SP 800-171 3.11.3 • CERT RMM v1.2 VAR:SG3.SP1	P1146 Develop and implement risk mitigation plans. • NIST CSF v1.1 ID.RA-6 • CERT RMM v1.2 RISK:SG5.SP1		P1152 Utilize an exception process for non-whitelisted software that includes mitigation techniques. • CMMC
			P1147 Manage non-vendor-supported products (e.g., end of life) separately and restrict as necessary to reduce risk. • CMMC		P1155 Analyze the effectiveness of security solutions at least annually to address anticipated risk to the system and the organization based on current and accumulated threat intelligence. • CMMC modification of NIST SP 800-171B 3.11.5e • CERT RMM v1.2 RISK:SG6.SP1

Crosswalk of CMMI V2 to CMMC

4: Very Close Match

- Audit and Accountability (Process Quality Assurance, Configuration Management)
- Recovery (Service View: Continuity)
- Awareness and Training (Organizational Training)

Domains from CMMC vs. **Practice Areas** in CMMI V2 matches:

5=Nearly Exact **4**=Very Close **3**=Partial **2**=Vague **1**=No Match

Crosswalk of CMMI V2 to CMMC

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)

Domains from CMMC vs. **Practice Areas** in CMMI V2 matches:

5=Nearly Exact **4**=Very Close **3**=Partial **2**=Vague **1**=No Match

Crosswalk of CMMI V2 to CMMC

2: Vague Match

- Maintenance (Continuity)
- Security Assessment (Strategic Service Management, Monitor and Control, Peer Review, Continuity, Incident Resolution and Prevention)
- Situational Awareness (Continuity, Incident Resolution and Prevention)

Domains from CMMC vs. **Practice Areas** in CMMI V2 matches:

5=Nearly Exact **4**=Very Close **3**=Partial **2**=Vague **1**=No Match

Crosswalk of CMMI V2 to CMMC

2: Vague Match (continued)

- Systems and Communications Protection (Strategic Service Management, Monitor and Control, Configuration Management)
- System and Information Integrity (Configuration Management, Incident Resolution and Prevention, Peer Reviews)

Domains from CMMC vs. **Practice Areas** in CMMI V2 matches:

5=Nearly Exact **4**=Very Close **3**=Partial **2**=Vague **1**=No Match

Crosswalk of CMMI V2 to CMMC

1: No Match

- Personnel Security
- Physical Protection

Domains from CMMC vs. **Practice Areas** in CMMI V2 matches:

5=Nearly Exact **4**=Very Close **3**=Partial **2**=Vague **1**=No Match

Example of No Match: Physical Protection

Domain = Physical Protection (PP)

Capability (C028)= Limit physical access

Maturity Level	Maturity Level Description	Processes
ML 1	Performed	*There are no maturity processes assessed at Maturity Level 1.* *An organization performs Level 1 practices but does not have process institutionalization requirements.*
ML 2	Documented	Establish a policy that includes [DOMAIN NAME].
		Document the CMMC practices to implement the [DOMAIN NAME] policy.
ML 3	Managed	Establish, maintain, and resource a plan that includes [DOMAIN NAME].
ML 4	Reviewed	Review and measure [DOMAIN NAME] activities for effectiveness.
ML 5	Optimizing	Standardize and optimize a documented approach for [DOMAIN NAME] across all applicable organization units.

CMMC Physical Protection

CMMC Model Appendices

B.13 Physical Protection (PE)

Physical Protection activities ensure that physical access to CUI asset containers is strictly controlled, managed, and monitored in accordance with CUI protection requirements.

The Physical Protection domain contains one capability:

1. Limit physical access

CMMC CLARIFICATION

You must supervise everyone who performs maintenance activities. Sometimes a person without proper permissions has to perform maintenance on your machines. Give that individual a logon that is active only once or for a very limited time, to limit system access.

Example

You are in charge of IT operations for your company. One of your software providers has to come on-site to update the software on your company's machines. You give the individual a temporary logon and password that expires in 12 hours. This gives him access long enough to perform the update. When he is on site, you remain with him. You supervise his activities. This ensures that he performs only the maintenance activities you directed.

REFERENCES

- NIST SP 800-171 Rev 1 3.7.6
- CERT RMM v1.2 TM:SG5.SP2
- NIST SP 800-53 Rev 4 MA-5

Using CMMI Expertise When No Overlap

Manage Physical Protection:

1. Determine requirements = **RDM** Requirements Development and Management
2. Create a protocol = **TS** Technical Solution or **PLAN** Planning
3. Control the protocol = **CM** Configuration Management
4. Train the users = **OT** Organizational Training
5. Make sure Physical Protection protocols are being followed = **MC** Monitoring and Control

Use the CMMI mechanisms you have in place for all areas of CMMC!

Summary

1) Using CMMI V2 can help you understand the requirements of CMMC. **Taxonomy** is very close in Levels, Domain/Practice Areas, and maturity requirements.
2) CMMI and CMMC both require **institutionalization**
3) Maturity levels are **cumulative** and **evolutionary**
4) For areas not closely covered by CMMI, there are other sources that can help an organization understand requirements such as (ISO 27001), NIST 800-171, CERT RMM, etc., that provide examples of what needs to be implemented.
5) **Reuse and extend your current expertise!**

Crosswalk of CMMC to CMMI V2

The entire Crosswalk will be available
www.ExcellenceinMeasurementTechnology.com
Excellence in Measurement Technology is
Margaret Tanner Glover CEO
Kieran Doyle President