Software Engineering Institute

Advancing Cybersecurity Capability Measurement Using the CERT®-RMM Maturity Indicator Level Scale

Matthew J. Butkovic
Richard A. Caralli

November 2013

TECHNICAL NOTE
CMU/SEI-2013-TN-028

CERT® Division

http://www.sei.cmu.edu

Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

This report was prepared for the
SEI Administrative Agent
AFLCMC/PZM
20 Schilling Circle, Bldg 1305, 3rd floor
Hanscom AFB, MA 01731-2125

DM-0000686

Table of Contents

List of Figures

List of Tables

Acknowledgments

The viability of the Maturity Indicator Level scale as a means measure security and resilience capabilities would not have been possible without the support and collaboration of our key partners. In particular, we would like to personally thank Jenny Menna, Director of the Stakeholder Engagement and Cyber Infrastructure Resilience division of the U.S. Department of Homeland Security, and Kevin Dillon, Branch Chief of Stakeholder Risk Assessment and Mitigation at DHS. Their advocacy for the development, piloting, and implementation of the Cyber Resilience Review has been essential to its success.

In addition, the authors would like to thank Samara Moore, the White House National Security Staff's Director for Cybersecurity and Critical Infrastructure Protection. Samara has been a champion of the development of maturity models in the energy sector, and Jason is continuing this effort by expanding their use in the oil and natural gas subsector. The authors would also like to thank Matthew Light, Cybersecurity Specialist at the North American Electric Reliability Corporation (NERC), whose extensive involvement in the development of the electricity subsector cybersecurity maturity model was critical to the adaptation of the MIL scale.

Finally, the authors would like to acknowledge Mark Knight, chair of the GridWise Architecture Council, who co-authored the "Maturity Models 101" white paper that helped to define and typify the various types of maturity models in the operational domain, and Austin Montgomery of the CERT Office of Communications and Transition for his unending support and advocacy for the development and deployment of improved cybersecurity practices in the energy sector. His enthusiasm has been a major factor in our collective success.

Executive Summary

In its simplest form, a *maturity model* is a set of characteristics, attributes, indicators, or patterns that represent progression and achievement in a particular domain or discipline. Architecturally, maturity models typically have levels arranged in an evolutionary scale that defines measurable transitions from one level of maturity to another. The current version of the CERT® Resilience Management Model (CERT®-RMM v1.2) utilizes the maturity architecture (levels and descriptions) as provided in the Capability Maturity Model Integration (CMMI) constellation models (Development, Acquisition, and Services) to ensure consistency with CMMI, particularly for CERT-RMM users who are already using one of the CMMI early lifecycle models. While the CMMI maturity levels and descriptions are a good fit for CERT-RMM, in practice the spacing between levels often causes CERT-RMM practitioners some difficulty. To address some of these issues, the CERT Division of the Software Engineering Institute, part of Carnegie Mellon University, did a comprehensive review of the existing specific and generic goals and practices in CERT-RMM to determine if a better scale could be developed to help users of the model show incremental improvement in maturity without breaking the original intent of the CMMI maturity levels. This resulted in the development of the maturity indicator level scale, or the CERT-RMM MIL scale.

Maturity indicator levels (MILs) are a specific representation of the capability levels currently instantiated in CERT-RMM. They describe attributes that would be *indicative* of these capabilities if the capabilities had been appraised through a formal appraisal process. In other words, achieving the MILs does not necessarily imply capability (as measured through formal CERT-RMM appraisal), but it does *indicate* capability.

While the MIL scale was originally prototyped in late 2011 as part of the planning for version 2.0 of CERT-RMM, the construct informed the development of hybrid maturity models—those that combine the progression of practices with the ability to measure increasing capability. The first application of the MIL scale was in the Cyber Resilience Review (CRR), a comprehensive review process based on CERT-RMM and developed in collaboration with the Department of Homeland Security to measure the effectiveness of resilience practices by owners and operators of critical infrastructure. Upon successful application in the CRR, the MIL scale was adapted for use in the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) developed collaboratively with the Department of Energy to comply with a White House initiative to examine and characterize the cybersecurity posture of the electric grid. The extensive piloting and use of the MIL scale in CRR and ES-C2M2 and the success of these models indicate that the MIL scale is not only a viable but accessible maturity architecture. Building on the success of ES-C2M2, the MIL scale is being incorporated into the Oil and Natural Gas Cybersecurity Capability Maturity Model (ONG-C2M2) and will form the basis for the maturity architecture of CERT-RMM v2.0.

® CERT® is a registered mark owned by Carnegie Mellon University.

Abstract

A *maturity model* is a set of characteristics, attributes, indicators, or patterns that represent progression and achievement in a particular domain or discipline. Maturity models typically have levels arranged in an evolutionary scale that defines measurable transitions from one level of maturity to another. The current version of the CERT® Resilience Management Model (CERT®-RMM v1.2) utilizes the maturity architecture (levels and descriptions) as provided in the Capability Maturity Model Integration (CMMI) constellation models to ensure consistency with CMMI. The spacing between maturity levels often causes CERT-RMM practitioners some difficulty. To address some of these issues, the CERT Division of Carnegie Mellon University's Software Engineering Institute did a comprehensive review of the existing specific and generic goals and practices in CERT-RMM to determine if a better scale could be developed to help users of the model show incremental improvement in maturity without breaking the original intent of the CMMI maturity levels. This technical note presents the results: the maturity indicator level scale, or CERT-RMM MIL scale.

1 A Quick Primer on Maturity Models

In its simplest form, a *maturity model* is a set of characteristics, attributes, indicators, or patterns[1] that represent progression and achievement in a particular domain or discipline. The artifacts that make up the model are typically agreed on by the domain or discipline, which validates them through application and iterative recalibration.

A maturity model allows an organization or industry to have its practices, processes, and methods evaluated against a clear set of artifacts that establish a benchmark. These artifacts typically represent best practice and may incorporate standards or other codes of practice that are important in a particular domain or discipline.

By having the ability to benchmark, organizations can use maturity models to determine their current level of achievement or capability and then apply these models over time to drive improvement. However, when used in a broader sense, maturity models can also help organizations benchmark their performance against other organizations in their domain or sector, and they can help an industry determine how well it is performing by examining the achievement or capability of its member organizations.

1.1 Architectural Constructs for Maturity Models

Architecturally, maturity models typically have levels arranged in an evolutionary scale that defines measurable transitions from one level to another. The corresponding attributes define each level; in other words, if an organization demonstrates these attributes, it is said to have achieved both that level and the capabilities that the level represents. Having measurable transition states between the levels enables an organization to use the scaling to

- define its current state
- define its future, more "mature" state
- identify the attributes it must attain to reach that future state

For instance, the Smart Grid Maturity Model (SGMM) [SEI 2012] assesses the progression of electricity utilities' smart grid maturity by evaluating many different attributes—from the utility's integration of new sensors, switches, and communications technologies for grid monitoring and control, to its extension of new control analytics across line-of-business decision making, to its having automated decision-making capabilities in place. The CERT® Resilience Management Model (CERT®-RMM), developed by the CERT Division of Carnegie Mellon University's Software Engineering Institute, bases the measurable transitions between maturity levels on the degree to which an organization has institutionalized a set of cybersecurity and

[1] This technical note refers to characteristics, attributes, indicators, and patterns as *attributes*.

® CERT® is a registered mark owned by Carnegie Mellon University.

resilience practices;[2] as an organization develops more mature capabilities, it advances through the levels.

For a maturity model to be effective and have impact, the measurable transitions between levels should be based on empirical data that have been validated in practice. That is, each step in the model should be provably more mature than the previous step. In essence, what constitutes mature behaviors must be characterized and validated, which can be challenging, if not impossible, to do unambiguously in many maturity models.

An effective, validated maturity model provides

- a place to start
- the benefit of a community's experience and knowledge
- a common language and a shared vision
- a way to define what improvement and maturity mean for an organization
- a framework for prioritizing actions
- a roadmap for increased maturity and return on investment (ROI)

1.2 Types of Maturity Models

In general, we have observed that maturity models can be categorized as one of the following three types [Caralli 2012]:

1. progression models
2. capability models
3. hybrid models

1.2.1 Progression Models

Progression maturity models represent a simple progression or scaling of a characteristic, indicator, attribute, or pattern in which the movement through the maturity levels indicates some progression of attribute maturity. This category includes many proprietary models developed by companies such as consultancies or product vendors, including the SEI's SGMM.

Progression models typically place their focus on the evolution of the model's core subject matter (such as practices or technologies) rather than attributes that define maturity (such as the ability and willingness to perform a practice, the degree to which a practice is validated, etc.). In other words, the purpose of a progression model is to provide a simple roadmap of progression or improvement as expressed by increasingly better versions (for example, more complete, more advanced) of an attribute as the scale progresses. For example, a simple maturity progression for counting might be

pencil and paper → *abacus* → *calculator* → *computer*

To put this in the context of actual security practices, a simple maturity progression for authentication might be

---

[2] *Institutionalization* refers to the degree to which something has become part of the culture, or "the way things are done" by the organization. Institutionalization depends on a number of factors such as documentation of the practice, assignments of roles and responsibilities, and the acquisition of appropriate skill sets.

simple passwords → *strong passwords* → *60-day change intervals* → *two-factor authentication* → *three-factor authentication*

In addition, in progression models, the maturity levels are often labeled relative to a state or step in the progression. In the counting example, level one might be expressed as *primitive*, and level three might be expressed as *tool enabled*.

Progression models are often described as being cast in the mold of a capability maturity model, but progression models do not typically measure capability or process maturity. In fact, an organization could demonstrate performance of more mature practices in a progression model, but it might be performing these practices in an ad hoc manner and be unable to obtain consistent results or retain these practices under stress. Therefore, achievement of more mature practices in a progression model *would not* indicate capability maturity.

1.2.2 Capability Maturity Models

In a capability maturity model (CMM), the dimension that is being measured is a representation of organizational capability around a set of characteristics, indicators, attributes, or patterns, often expressed as *processes*.[3] This is important because a CMM measures more than the ability to perform a task: a CMM also focuses on broader organizational capabilities that reflect the maturity of the culture and the degree to which the capabilities are embedded (or institutionalized) in the culture. Thus, the levels in a CMM describe states of organizational maturity relative to process maturity such as

ad hoc → *managed* → *defined* → *quantitatively managed* → *optimized*

Because of the generic nature of process maturity scaling, the basic maturity carriage of the CMMI framework can be applied to other domains, such as service management and operational resilience. As a result, operations-focused[4] models such as CMMI for Services and CERT-RMM have emerged to take advantage of this time-proven means for improving performance.

1.2.3 Hybrid Models

Hybrid maturity models merge two abilities: the ability to measure maturity attributes and the ability to measure evolution or progression in progressive models. This type of model reflects transitions between levels that are similar to capability model levels (i.e., that describe capability maturity) but also account for the evolution of attributes in a progression model. Hybrid models are very useful for focusing on specific subject matter domains as well as assessing how well standards and best practices have been included in the organization's capabilities. By adding a means to measure capability, hybrid models become relatively easy to use and understand, have great value, and can be used as roadmaps to improved maturity. In other words, hybrid models provide the rigor of capability maturity models while embracing the ease of use and comprehensibility of progression models.

---

[3] Indeed, CMMs are often referred to as *process models*.

[4] CMMI for Development and CMMI for Acquisition focus on early lifecycle development and acquisition activities, and operations-focused capability maturity models focus on processes that are by nature continuous (i.e., they are performed continuously and may overlap).

One example of a hybrid model is the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) [DOE 2012], which was developed by applying the capability maturity concepts in CERT-RMM to existing codes of practice in the energy sector. ES-C2M2 also incorporates an enhanced maturity scaling, which is the subject of this technical note.

1.3 Essential Components of a Maturity Model

Despite the differences between types of maturity models, most of them conform to some structural basics. This structure is important because it provides a linkage between objectives, assessments, and best practices, and it facilitates relationships between current capabilities and improvement roadmaps by linking them to business goals, standards, and other criteria.

1.3.1 Levels

As previously discussed, levels represent the transitional states in a maturity model. Depending on the architecture, a model's levels may describe a progressive step or plateau, or they may represent an expression of capability or other attribute that can be measured by the model. Levels are important because they represent the measurement aspect of a maturity model, and if the scaling is inaccurate or incomplete, the model itself may not be able to be validated or will produce poor or inconsistent results. For this reason, the term *maturity model* must be used with caution and applied only to models that actually adhere to the characteristics of maturity models, especially CMMs, which have much more rigorous and empirically valid leveling.

1.3.2 Model Domains

Model domains essentially define the scope of a maturity model. Domains are a means for grouping like attributes into an area of importance for the subject matter and intent of the model. In capability maturity models, the domains are often (but not necessarily) referred to as *process areas* because they are a collection of processes that make up a larger process or discipline (such as software engineering). Depending on the model, users may be able to focus on improving a single domain or a group of domains. Some models, such as the CMMI framework, might contain a representation that requires a prescribed progression through the domains to achieve the intended result.[5]

1.3.3 Attributes

Attributes represent the core content of the model and are grouped by domain and level. In other words, attributes are defined at the intersection of a domain and a maturity level. They are typically based on observed practice, standards, or other expert knowledge and can be expressed as characteristics, indicators, practices, or processes. In capability maturity models, attributes typically also express qualities of organizational maturity (such as planning and measuring) that are important for supporting process improvement regardless of the process being modeled.

---

[5] The CMMI framework contains *continuous* and *staged* model representations. Continuous representations address an individual process area and its measurement of capability. Staged representations prescribe a path through the process areas, group process areas together, and can express organizational maturity as capability improves across the group.

1.3.4 Appraisal and Scoring Methods

Appraisal and scoring methods, based on the model, facilitate assessment. They can be formal or informal, expert-led or self-applied. Scoring methods are algorithms devised by the community to ensure consistency of appraisals and a common standard for measurement. Scoring methods can include weighting (so that important attributes are valued over less important ones) or can value different types of data collection in different ways (such as providing higher marks for documented evidence than for interview-based data).

1.3.5 Improvement Roadmaps

In addition to being used for benchmarking, maturity models can be used to guide improvement efforts. Many of these models have prescribed methods for identifying an improvement scope, diagnosing current state, planning and implementing improvement activities, and verifying that improvement has occurred. These methods define a classic plan-do-check-act (PDCA) cycle that incorporates a maturity model as the basis for the improvement, so maturity models are often referred to in a larger construct called *model-based process improvement*. The IDEAL[SM] model is a reference model for using the CMMI framework in a PDCA cycle[6] and can be used to guide any model-based process improvement effort.

[SM] IDEAL is a service mark of Carnegie Mellon University.

[6] For more information on the IDEAL model, go to http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=12449.

2 Introducing the Maturity Indicator Level (MIL) Concept

2.1 Introduction

The current version of CERT-RMM (v1.2) utilizes the maturity architecture (levels and descriptions) as provided in the CMMI constellation models (Development, Acquisition, and Services) to ensure consistency with CMMI, particularly for CERT-RMM users who are already using one of the CMMI early lifecycle models. There were many drivers for this decision:

- CERT-RMM could take advantage of a proven maturity scaling whose large installed user base had extensively piloted and refined its use.
- By staying consistent with CMMI models, existing CMMI users would be able to more quickly adopt CERT-RMM for their operational needs.
- CMMI users could combine CMMI early lifecycle models with CERT-RMM to form a comprehensive process improvement approach across *all* phases of the lifecycle, rather than ending the improvement activities as assets were implemented.
- Maturity levels in CMMI address the degree to which good practices are retained in times of stress. The ability to retain good practices under stress is a major driver for practitioners in the security and resilience fields because disruption is often characterized by uncertainty regarding the viability of essential functions.

2.1.1 Drivers for Developing a New Maturity Scale

While the CMMI maturity levels and descriptions are a good fit for CERT-RMM, in practice the spacing between levels often causes CERT-RMM practitioners some difficulty. This is mostly because the ability to move from one level to another is a tremendous commitment that often does not reflect incremental improvements that are being achieved by the practitioners.

Through classroom experience and in coaching users of CERT-RMM, we have observed some confusion over the fact that many capabilities that lead to maturity are embedded in specific practices rather than generic practices, even though they appear to be a primary stepping stone that traverses many of the process areas in the model. An example of this problem is in found in the *planning* activity that is observed in many CERT-RMM process areas. Planning as an activity is usually considered to be a basic function (hence it is included in CMMI models as a specific goal or practice), yet it can be an indication that an organization is making an attempt to improve a process by at least developing requirements in advance of having to implement the process during a disruption. Thus, in CERT-RMM, the planning activity appears to imply a higher level of maturity that is not specifically called out in the current CMMI or CERT-RMM maturity scaling.

Another observation is that the existing *managed* level includes many functions that organizations typically do not do together or take on simultaneously in an improvement process. In the current *managed* level, the organization is asked to make a commitment to no less than

- governing the process
- planning the process

- resourcing the process
- training the process participants
- managing work products
- including stakeholders in the process
- monitoring and controlling the process
- measuring the process
- including high-level managers in the process

Achieving each of these activities separately appears to help organizations move in an incrementally positive direction toward higher process maturity, yet they get no credit for improvement unless they have performed all of these activities as a group. This impedes model adoption because organizations are not likely to take on improvement efforts if they must make large resource commitments for what appears to be only a one-level improvement.

Finally, we also observed that models derived from CERT-RMM for specific purposes were not easily able to implement the current maturity scale. Specifically, this problem occurs because some users of CERT-RMM attempt to apply maturity scaling to each specific practice in a process area, rather than to the collection of specific practices as a group. In other words, users might want to measure the maturity of their inventory assets process (ADM:SG1.SP1) rather than all of the specific goals and practices in Asset Management (ADM).

To address some of these issues, we did a comprehensive review of the existing specific and generic goals and practices in CERT-RMM to determine if a better scale could be developed to help users of the model show incremental improvement in maturity without breaking the original intent of the CMMI maturity levels. This resulted in the development of the maturity indicator level scale, or the CERT-RMM MIL scale.

In Appendix A and Appendix B, we demonstrate how this new scaling has been applied to widely used models derived from CERT-RMM.

3 Defining the Maturity Indicator Levels

3.1 Introduction

Maturity indicator levels are a specific representation of the capability levels currently instantiated in CERT-RMM. They describe attributes that would be *indicative* of these capabilities if the capabilities had been appraised through a formal appraisal process. In other words, achieving the MILs does not necessarily imply capability (as measured through formal CERT-RMM appraisal), but it does *indicate* capability. Therefore, the MIL scale is highly useful when focusing on improvement as opposed to assigning a capability level.[7]

As a refresher, the current capability levels in CERT-RMM are

- Capability Level 0: Incomplete
- Capability Level 1: Performed
- Capability Level 2: Managed
- Capability Level 3: Defined

In the MIL scale, the maturity indicator levels are:

- MIL0 Incomplete
- MIL1 Performed
- MIL2 Planned
- MIL3 Managed
- MIL4 Measured
- MIL5 Defined
- MIL6 Shared

For comparison purposes, the MIL scale can be mapped to the existing capability levels in CERT-RMM. This could be useful for organizations that have already begun using CERT-RMM but want to adopt the MIL scale in future applications.

Table 1: Mapping of CERT-RMM Capability Levels to the MIL Scale

CERT-RMM Capability Level	MIL
Level 0: Incomplete	MIL0: Incomplete
Level 1: Performed	MIL1: Performed
Level 2: Managed	MIL2: Planned[8] MIL3: Managed MIL4: Measured[9]
Level 3: Defined	MIL5: Defined
	MIL6: Shared[10]

[7] The MIL scale was originally developed as a new feature of CERT-RMM version 2.0, which is currently in the planning stage.

[8] MIL2 Planned is newly added to the original CMMI-based capability levels.

[9] MIL4 Measured is newly added to the original CMMI-based capability levels.

The following sections define each CERT-RMM MIL and propose a set of questions that can be used to test for indicators of maturity at each level, as applied to specific practices in the model.

3.1.1 MIL0 Incomplete

MIL0 Incomplete indicates that a specific practice in a CERT-RMM process area[11] is not being performed. If MIL0 is assigned, no further assessment of maturity indicator is performed because incomplete processes are not institutionalized.

3.1.1 MIL1 Performed

MIL1 Performed indicates that a specific practice in a CERT-RMM process area is being performed. MIL1 means that there is sufficient and substantial support for the existence of the practice. Once MIL1 is attained, questions related to higher MILs can be asked to determine if the practice is institutionalized to higher degrees of maturity.

3.1.1 MIL2 Planned

MIL2 Planned indicates that a specific practice in a CERT-RMM process area is not only performed but is supported by sufficient planning, stakeholders, and relevant standards and guidelines. A planned process or practice is

- established by the organization
- planned
- supported by stakeholders
- supported by relevant standards and guidelines

3.1.1 MIL3 Managed

MIL3 Managed indicates that a specific practice in a CERT-RMM process area is performed, is planned, and has the basic infrastructure in place to support the process. A managed process or practice

- is governed by the organization
- is appropriately staffed and funded
- is assigned to staff who are responsible and accountable for the performance of the practice
- is performed by staff who are adequately trained to perform the practice

---

[10] MIL6 is an experimental MIL that does not map to any existing CERT-RMM capability level. It is intended to address maturity of a practice that traverses various constituencies in a community for the overall improvement of the community. For example, sharing an incident management process across many different energy companies that share different operating territories could improve the overall resilience of the power supply during a disruption, particularly if the process is consistent and repeatable regardless of which organization performs it.

[11] "Specific practice in a CERT-RMM process area" refers to a core practice in the CERT-RMM model. For example, in the Asset Definition and Management process area, Inventory Assets would be considered a core or specific practice. To apply the MIL scale to another model, it can be useful to substitute "CERT-RMM process area" with a domain or category and "specific practice" with a practice, technology, or attribute. At MIL0 for example, the practice, technology, or attribute would be non-existent or not observed, indicating that the practice is not performed or the technology has not been implemented.

- produces work products that are expected from performance of the practice and are placed under appropriate levels of configuration control
- is managed for risk

3.1.1 MIL4 Measured

MIL4 Measured indicates that a specific practice in a CERT-RMM process area is performed, planned, managed, monitored, and controlled. A measured process or practice is

- periodically evaluated for effectiveness
- monitored and controlled
- objectively evaluated against its practice description and plan
- periodically reviewed with higher level management

3.1.1 MIL5 Defined

MIL5 Defined indicates that a specific practice in a CERT-RMM process area is performed, planned, managed, monitored, controlled, and consistent across all internal[12] constituencies who have a vested interest in the performance of the practice. A defined process or practice ensures that the organization reaps the benefits of its consistent performance across organizational units and that all organizational units can benefit from improvements realized in any organizational unit. At MIL5, a process or practice

- is defined by the organization and tailored by individual operating units within the organization for their use
- is supported by improvement information that is collected by and shared among operating units for the overall benefit of the organization

3.1.1 MIL6 Shared

MIL6 Shared indicates that a specific practice in a CERT-RMM process area is performed, planned, managed, monitored, controlled, and consistent across all internal and external[13] constituencies who have a vested interest in the performance of the practice. A shared process or practice ensures that the *community* reaps the benefits of consistent performance of the practice across many organizations bound by the community (for example, because they collectively provide a shared service such as power generation in a geographical region) and that all of the community's organizations can benefit from improvements realized in any community organization. At MIL6, a process or practice is

- defined by the community and tailored by that community's organizations for their use
- supported by improvement information that is collected by and shared among organizations for the overall benefit of the community

---

[12] In this case, "internal" refers to constituencies over which the organization has direct managerial control.

[13] In this case, "external" refers to constituencies over which the organization does not have direct managerial control.

4 Applying the MIL Scale

The CERT-RMM MIL scale can be used for any assessment-based instrument derived from CERT-RMM. It can also be applied to any other assessment instrument where an indicator of process maturity and institutionalization is helpful in describing the degree to which the process or practice is retained under times of stress and whose outcomes must be consistent, repeatable, and of high quality.

When applying the MIL scale for CERT-RMM, it is most appropriate to focus at the specific practice level, such as "ADM:SG1.SP1 Inventory Assets."[14] For example, to determine if the specific practice "ADM:SG1.SP1 Inventory Assets" is being performed, the descriptions of each of the MILs would be applied to determine the indicated level of maturity of the practice. In addition, as in all models built on the CMMI architecture, the MIL scale is cumulative; thus, if you are testing a practice for a particular MIL, the practice needs to have already achieved the previous MILs.

4.1 Determining the Appropriate Maturity Indicator Level

In the most informal way, determining the appropriate MIL is a function of determining if the basic intent of the level is observable and verifiable in the model characteristic (practice, attribute, technology, etc.) being inspected. To aid in applying the scale, the following questions can be used to make a determination about the appropriate level of performance. Remember, MILs are cumulative, so for MILs 1 and above, the previous MILs need to have been achieved.

MIL1

- Is there evidence that the practice is being performed?
- Are the basic expected outputs of the practice observable and available for inspection?

MIL2

- Has MIL1 been achieved?
- Is the practice documented and communicable to all who need to know?
- Is the practice performed according to a documented plan?
- Are the stakeholders of the practice known, and are they aware of the practice and their role in it?
- Have the standards and guidelines that support the practice been identified and implemented?

MIL3

- Have MIL1 and MIL2 been achieved?
- Is the practice supported by policy, and is there appropriate oversight over the performance of the practice?

[14] Refer to *CERT® Resilience Management Model* [Caralli 2011, pg. 49] for an explanation of the nomenclature for specific practices in CERT-RMM.

- Are the staff and funds that are necessary to perform the practice as intended available?
- Have staff been assigned to perform the practice, and are they responsible and accountable for its performance?
- Are the staff who perform the practice adequately skilled and trained to perform it?
- Does the practice produce artifacts and work products that are expected from it performance, and if so, are the configurations of these artifacts and work products managed?
- Are risks related to the performance of the practice identified, analyzed, disposed of, monitored, and controlled?

MIL4

- Have MIL1, MIL2, and MIL3 been achieved?
- Is the practice periodically reviewed to ensure that it is effective and producing intended results?
- Are appropriate implementation and performance measures identified, applied, and analyzed?
- Is the practice periodically evaluated to ensure that it adheres to the practice description and the plan for the practice?
- Is higher level management aware of any issues related to the performance of the practice?

MIL5

- Have MIL1, MIL2, MIL3, and MIL4 been achieved?
- Is there an organization-sponsored definition of the practice from which operating units can derive practices that fit their unique operating circumstances?
- Are practice improvements documented and shared across internal constituencies so that the organization as a whole reaps benefits from these improvements?

MIL6

- Have MIL1, MIL2, MIL3, MIL4, and MIL5 been achieved?
- Is there a community-sponsored definition of the practice from which organizations can derive practices that fit their unique operating circumstances while still achieving the shared goals of the community?
- Are practice improvements documented and shared across organizations so that the community as a whole benefits from these improvements?

Appendix A Application of the MIL Scale in the Cyber Resilience Review (CRR)

Background

The Cyber Resilience Review (CRR) is a lightweight assessment method derived from the CERT-RMM version 1.1. It was created in collaboration with the Department of Homeland Security for the purpose of evaluating the cybersecurity and service continuity practices of critical infrastructure owners and operators. The CRR questionnaire, containing 269 questions, is delivered in a six-hour facilitated workshop setting. Answers are elicited from cybersecurity, operations, physical security, and business continuity personnel within critical infrastructure organizations. The CRR has been used to examine more than 200 organizations within 12 of the 16 critical infrastructure sectors.[15]

CRR Architecture

The CRR comprises 42 goals and 139 specific practices extracted from the CERT-RMM and organized in 10 domains:

1. Asset Management
2. Controls Management
3. Configuration and Change Management
4. Vulnerability Management
5. Incident Management
6. Service Continuity Management
7. Risk Management
8. External Dependencies Management
9. Training and Awareness
10. Situational Awareness

Similar to CERT-RMM process areas, each domain in the CRR includes

- a purpose statement that explains the scope and intent of the domain
- specific goals that describe the unique capabilities that characterize the domain
- specific practices that support the achievement of the domain's goals and align with the domain's purpose statement
- common goals that define each of the MILs
- common practices that represent institutionalizing features as defined in CERT-RMM

Figure 1 depicts these architectural constructs.

[15] As defined in Presidential Policy Directive 21 (PPD-21, see http://www.dhs.gov/critical-infrastructure-sectors).

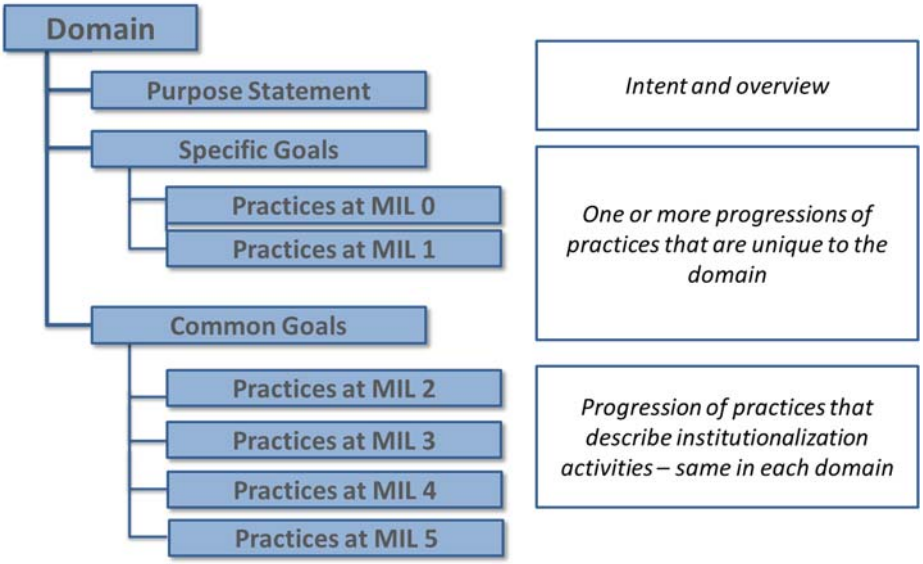

Figure 1: CRR Domain Architecture

Applying the MIL Scale in the CRR

Unlike ES-C2M2, which deploys a hybrid architecture to measure domain progress and capability maturity, the CRR more closely aligns with the capability maturity architecture of CERT-RMM. In this architecture, a core set of goals and practices—referred to as *specific goals and practices* in CERT-RMM—defines the basic knowledge and skills that must be demonstrated in the domain. The capability maturity dimension is represented by a generic set of goals and practices that indicate increasing levels of capability for performing the core set of goals and practices. Thus, in the CRR, the maturity dimension is singularly measured by the MIL scale.

The CRR applies the MIL scale as it is defined in CERT-RMM version 2.0: six levels, from MIL0 (Incomplete) to MIL5 (Defined).[16] To determine the degree to which the core set of goals and practices are being institutionalized, the CRR asks a common set of 13 MIL questions for each of the 10 CRR domains. Table 2 shows how the MIL scale is applied to the CRR.

[16] It was determined that the length and pace of the CRR did not permit an adequate evaluation of practices at MIL6 (Shared).

Table 2: MILs in the CRR

Level	Name	Description/Attributes
MIL0	Incomplete	• Practices in a domain are not being fully performed.
MIL1	Performed	• Practices in a domain are being performed.
MIL2	Planned	• Domain activities are documented in a plan. • Stakeholders are involved and aware of their roles. • Standards or guidelines are used to guide practice implementation.
MIL3	Managed	• Management oversees performance of domain activities. • Qualified staff have been assigned to perform domain activities. • Adequate funding is provided to perform domain activities. • Risks related to performance of domain activities is identified and managed.
MIL4	Measured	• Domain activities are periodically reviewed and measured for effectiveness. • Domain activities are periodically reviewed to ensure they are adhering to the plan. • Higher level management is aware of issues related to the performance of domain activities.
MIL5	Defined	• A standard definition of domain activities has been adopted from which operating units can derive practices that fit their unique operating circumstances. • Improvements to domain activities are documented and shared across the organization.

Measuring Performance in the CRR

The CRR measures performance of an organization at the practice, goal, domain, and MIL levels. Scores are calculated for each of individual model elements and in aggregated totals. The scoring rubric establishes the following:

- Practices can be observed in one of three states: performed, incomplete, and not performed.
- A domain goal is achieved only if all of the practices related to the goal are achieved.
- A domain is fully achieved only if all the goals in the domain are achieved.

As in CERT-RMM, if the above conditions are met, the organization is said to be achieving the domain in a *performed* state: the practices that define the domain are observable, but no determination can be made about the degree to which these practices are

- repeatable under varying conditions
- consistently applied
- able to produce predictable and acceptable outcomes
- retained during times of stress

These conditions are tested for by applying a common set of 13 MIL questions to the domain, but only after MIL1 is achieved. Consistent with the architecture of the MIL scale, MILs are cumulative; to achieve a MIL in a specific domain, an organization must perform all of the practices in that level and in the preceding MILs. For example, an organization must perform all of the domain practices in MIL1 and MIL2 to achieve MIL2 in the domain.

CRR participants receive a comprehensive report containing results for each question in all domains. The report also provides graphical summaries of the organization's performance at the goal and domain levels, depicted in a heat-map matrix (Figure 2). The colors indicate

achievement (green), partial achievement (yellow), and failure to achieve (red). This detailed representation allows organizations to target improvement at a fine-grained level.

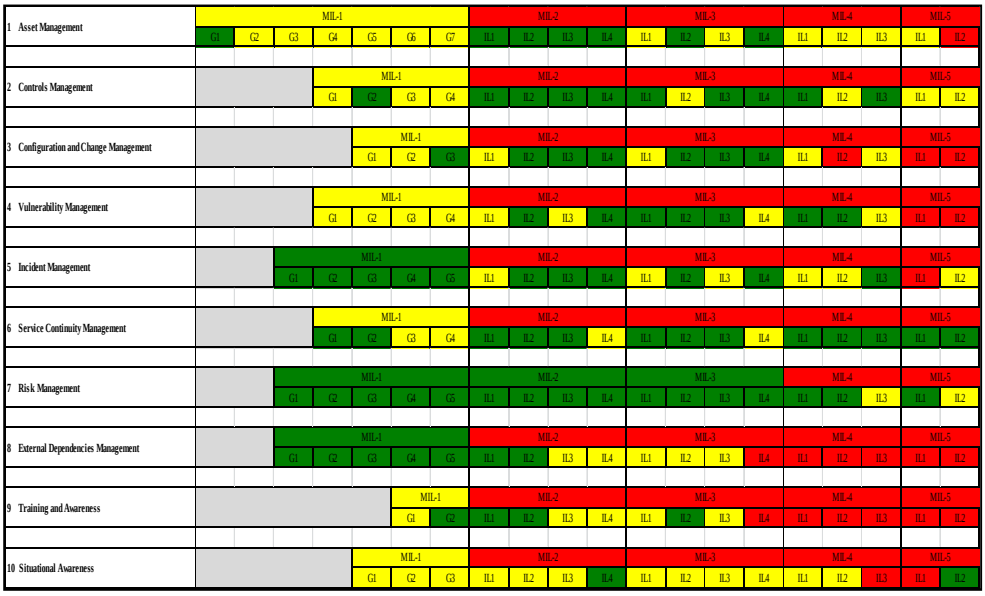

Figure 2: Example of CRR Heat Map

CRR reports also summarize MIL performance by domain (Figure 3).

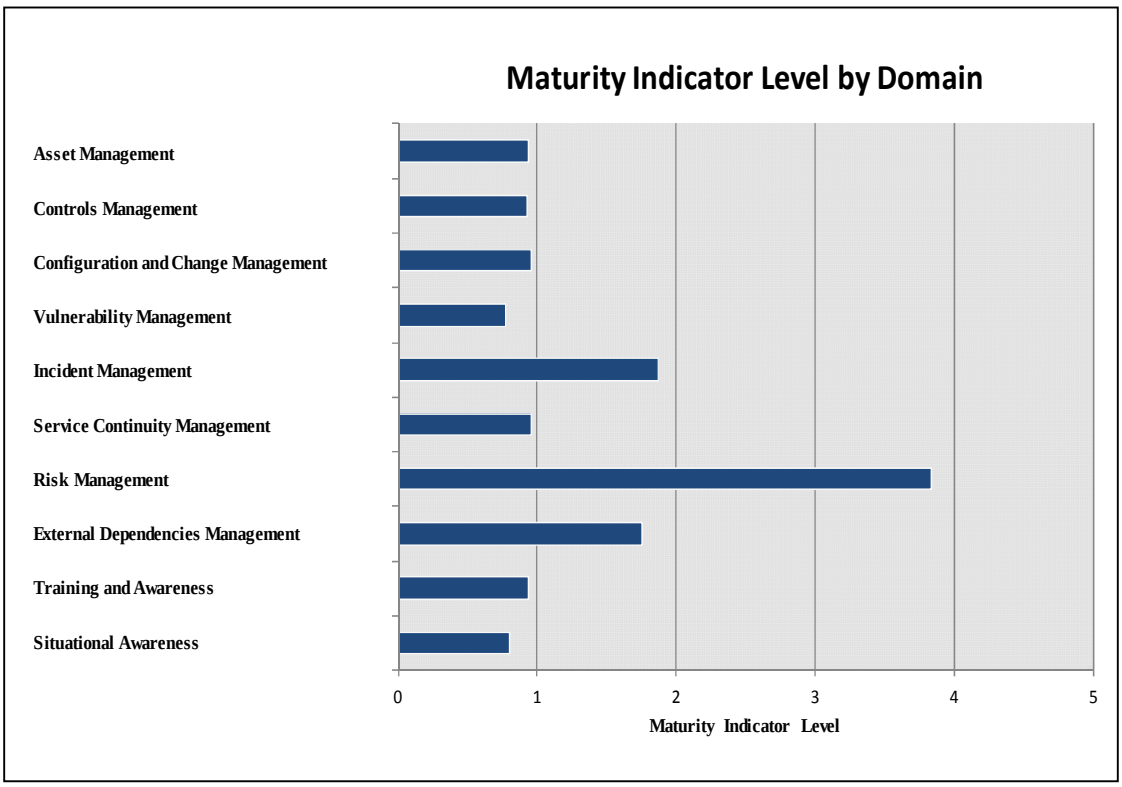

Figure 3: Example of MIL Graph

Appendix B Application of the MIL Scale in the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)

Background

In response to a 2011[17] White House initiative to examine and characterize the cybersecurity posture of the electric grid, the Department of Energy commissioned the development of the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) [DOE 2012]. Through collaboration among electricity utility owners and operators, private-sector subject matter experts, national laboratories, academia, and federal agencies, the model has become a useful and practical way to benchmark cybersecurity activities and the degree to which these activities are institutionalized. Higher degrees of institutionalization *can* result in improved ability to manage, direct, and control the protection and sustainability of key organizational assets under stress.

To meet the White House's requirements, the project team decided to develop a maturity model. Much of the background on maturity models presented early in this document was provided to the project team to help it decide on a model architecture that would not only convey best practices from a maturity perspective but also be simple to implement and use over time. However, the team had a strong desire to be able to measure capability maturity without the more rigorous requirements of CERT-RMM, from which some of the basic structure of ES-C2M2 is derived. In response, CERT personnel developed a hybrid maturity model architecture to meet these requirements. Further, to provide the ES-C2M2 model with a useful approximation of the capability maturity dimension from CERT-RMM, the project team adapted the MIL scale developed by for CERT-RMM v2.0.[18]

Integrating the MIL scale into the ES-C2M2 provides an important benefit to utilities. While the community identified the key practices that are most important to protecting the nation's electricity infrastructure, the MIL scale allows users to measure the degree to which these practices are institutionalized within an organization, revealing potential weaknesses. As a hybrid model, ES-C2M2 allows users to measure both the degree to which advanced practices and technologies are deployed and the degree to which these advancements are ingrained in the way an organization operates. This is important because disruptive and stressful conditions often occur without warning, and organizations must be able to respond in a consistent and repeatable way with predictable outcomes.

Model Architecture

ES-C2M2 includes 10 domains, which represent logical groupings of practices that model participants identified as important for utilities to perform. For ease of application, these domains

[17] See http://www.whitehouse.gov/blog/2012/01/09/protecting-nation-s-electric-grid-cyber-threats?utm_source=related.

[18] CERT-RMM v2.0 is currently in development. The MIL scale was developed in late 2011 in anticipation of the development of CERT-RMM v2.0.

have been given simple identifiers such as “Risk” or “Dependencies.” Figure 4 illustrates the full range of domains. More information on the domains can be found in the ES-C2M2 model.

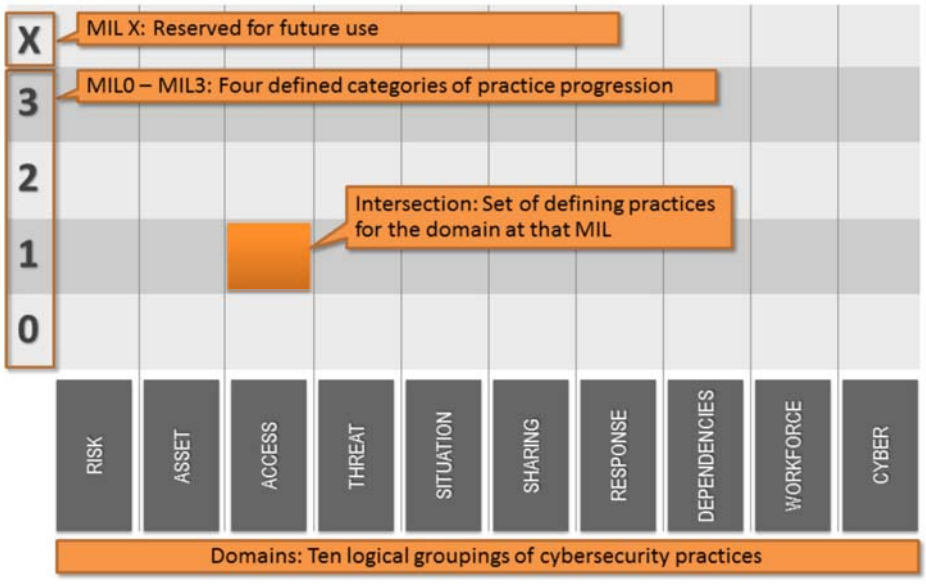

Figure 4: Domains of the ES-C2M2

Each domain has been developed to have a common architecture (Figure 5), which includes

- a purpose statement that summarizes the domain
- introductory notes that provide context and examples of how the domain might be applied within a utility
- one or more specific objectives (depending on the domain) that connect individual practices to the domain’s purpose statement
- specific practices that are categorized under specific objectives. These practices are unique to the domain, although some practices rely on specific practices from other domains. For example, in the Risk Management domain, a specific practice is to “Create and use a risk register for identified risks.” In the Threat and Vulnerability Management domain, the risk register is connected to analyzing and remediating identified threats and vulnerabilities.
- a common objective that consists of institutionalizing practices across each domain. These institutionalizing practices represent the capability maturity dimension that was transitioned from CERT-RMM to create the hybrid model.

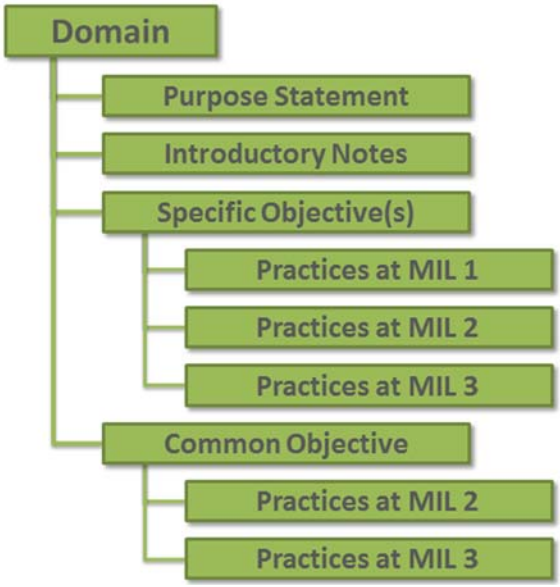

Figure 5: ES-C2M2 Domain Architecture

Application of the CERT-RMM MIL Scale

In ES-C2M2, the CERT-RMM MIL scale is applied as four MILs: MIL0 through MIL3. The practices in each domain are arranged in each of these four levels. The name of each MIL describes the level of capability that is attained by achieving both the domain practices *and* the practices that represent institutionalization of the domain practices. In other words, at each MIL, an organization is demonstrating two important attributes:

1. accomplishment of practices that represent maturity in the domain
2. accomplishment of practices that represent improving capability to apply these domain practices in a consistent and repeatable way, retain these practices under times of stress, and obtain consistent outcomes from the application of these practices

As organizations advance through the MILs, they demonstrate more mature and advanced domain knowledge and skill as well as improved capabilities to retain and apply this knowledge.

As in most maturity models, advancement up the MILs is a cumulative process (requiring that practices in previous MILs are achieved and maintained), and an organization can have a different MIL in each domain. For example, an organization may attain MIL2 in the Risk domain but MIL3 in the Threat domain. This may be acceptable given the organization's unique operating circumstances.

Table 3 provides descriptions of each ES-C2M2 MIL as well as a comparison to the CERT-RMM MIL scale.

Table 3: MILs in the ES-C2M2

Level	Level Name	Relationship to Original MIL Scale Level	Description
MIL0	Not Performed[19]	Incomplete	• Practices are not performed.
MIL1	Initiated[20]	Essentially defined by the "Performed" level	• Initial practices are performed, but may be ad hoc.
MIL2	Performed[21]	Essentially defined by the "Planned" level	• Practices are documented. • Stakeholders are involved. • Adequate resources are provided for the practices. • Standards or guidelines are used to guide practice implementation. • Practices are more complete or advanced than at MIL1.
MIL3	Managed[22]	Consistent with the "Managed" level, but with fewer requirements	• Domain activities are guided by policy (or other directives). • Activities are periodically reviewed for conformance to policy. • Responsibility and authority for practices are clearly assigned to personnel with adequate skills and knowledge. • Practices are more complete or advanced than at MIL2.

Ultimately, in the ES-C2M2, the application of the CERT-RMM MIL scale enables the development and deployment of a hybrid maturity model that provides a way to measure both domain knowledge and skill as well as capability. This innovation provides the benefits of traditional capability maturity models in a more agile and easily implementable process.

---

19 The original MIL scale describes this level as *Incomplete*.

20 The original MIL scale describes this level as *Performed*. A practice that is performed may be done in an inefficient or ineffective way (ad hoc) and still produce the intended result. However, the practice may not be reliable under stressful conditions, may not be repeatable or consistent over time, and may require human intervention to be effective.

21 The original MIL scale describes this level as *Planned*.

22 This level is a scaled-down version of the *Managed* level as defined in the original MIL scale.

References

URLs are valid as of the publication date of this document.

[Caralli 2011]
Caralli, Richard A.; Allen, Julia H.; & White, David W. *CERT® Resilience Management Model: A Maturity Model for Managing Operational Resilience.* Addison-Wesley, 2011.

[Caralli 2012]
Caralli, Richard A. *Discerning the Intent of Maturity Models from Characterizations of Security Posture.* Software Engineering Institute, Carnegie Mellon University, 2012. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=58922

[DOE 2012]
U.S. Department of Energy & U.S. Department of Homeland Security. *Electricity Subsector Cybersecurity Maturity Model.* Carnegie Mellon University, 2012. http://energy.gov/sites/prod/files/Electricity%20Subsector%20Cybersecurity%20Capabilities%20Maturity%20Model%20%28ES-C2M2%29%20-%20May%202012.pdf

[SEI 2012]
Software Engineering Institute. *Smart Grid: Tools and Methods.* http://www.sei.cmu.edu/smartgrid/tools/ (2012).

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	November 2013	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Advancing Cybersecurity Capability Measurement Using the CERT®-RMM Maturity Indicator Level Scale	FA8721-05-C-0003

6. AUTHOR(S)

M.J. Butkovic, R. A. Caralli

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2013-TN-028

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116	n/a

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

A *maturity model* is a set of characteristics, attributes, indicators, or patterns that represent progression and achievement in a particular domain or discipline. Maturity models typically have levels arranged in an evolutionary scale that defines measurable transitions from one level of maturity to another. The current version of the CERT® Resilience Management Model (CERT®-RMM v1.2) utilizes the maturity architecture (levels and descriptions) as provided in the Capability Maturity Model Integration (CMMI) constellation models to ensure consistency with CMMI. The spacing between maturity levels often causes CERT-RMM practitioners some difficulty. To address some of these issues, the CERT Division of Carnegie Mellon University's Software Engineering Institute did a comprehensive review of the existing specific and generic goals and practices in CERT-RMM to determine if a better scale could be developed to help users of the model show incremental improvement in maturity without breaking the original intent of the CMMI maturity levels. This technical note presents the results: the maturity indicator level scale, or CERT-RMM MIL scale.

14. SUBJECT TERMS	15. NUMBER OF PAGES
maturity models, capability maturity models, cybersecurity maturity models, cybersecurity measurement and analysis	37

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL