Everything You Always Wanted to Know About Maturity Models

Dr. Nader Mehravari
Research Scientist, CERT® Division

Dr. Nader Mehravari is with the CERT® Program at the Software Engineering Institute (SEI), a unit of Carnegie Mellon University in Pittsburgh, PA. His current areas of interest and research include operational resilience, protection and sustainment of critical infrastructure, preparedness planning, and associated risk management principles and practices.

Nader was with Lockheed Martin from 1992 through 2011. In his most recent assignment, he was the Director for Business Resiliency. In this capacity, he led and oversaw all preparedness planning and associated governance and compliance activities. He was responsible for building and leading Lockheed Martin's resiliency program where he successfully implemented a modern, integrated, risk management based approach to disaster recovery, business continuity, pandemic planning, crisis management, emergency management, and workforce continuity for all of Lockheed Martin.
Notices

Copyright 2014 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.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon® and CERT® are registered marks of Carnegie Mellon University.

DM-0000899
Outline

Setting the Stage
- The need for “measuring” operational activities & their effectiveness
- Are we doing the right things?
- Are we using the right tools to measure?
- Are we measuring the right things?

ABCs of Maturity Models
- What are Maturity Models?
- Types of Maturity Models
- Examples of Maturity Models

Closing Thoughts
- A few cautions
- Determining when and which type to use
Setting the Stage

- The need for “measuring” operational activities & their effectiveness
- Are we doing the right things?
- Are we using the right tools to measure?
- Are we measuring the right things?
Today’s Operating Environment

Rapid changes in technology and its application in a wide range of industries.

Introduction of many new systems, business processes, markets, risks, and enterprise approaches.

Many immature products and services being consumed by enterprises that themselves are in a state of change.
Challenges at Hand

- How can you tell if you are doing a good job of managing these changes?
- How best to monitor your progress on an ongoing basis?
- How do you manage the interactions of systems and processes that are continually changing?
- How do poor processes impact interoperability, safety, reliability, efficiency, and effectiveness?
Which tool should I use?

Your organization wants to know **SOMETHING** about your mission operation:

- How **EFFECTIVE** are we?
- Do we have the right **SKILLS** and **CAPABILITIES**?
- Do we have the right **TECHNOLOGIES**?

**OR**
Observation

The development and use of maturity models in security, continuity, IT operations, & resilience space is increasing dramatically.
Do maturity models measure the right thing?

- **May not measure what you think it measures**
  - Practice maturity vs. organizational maturity?

- **May give you inaccurate data on which to base decisions**
  - Process performance vs. product performance?

- **Can increase cost but reduce benefit**
  - An improved process may not result in compliance

- **May provide a false sense of confidence**
  - A robust process may not stop all malware
ABCs of Maturity Models

- What are Maturity Models?
- Types of Maturity Models
- Examples of Maturity Models
Maturity Model Defined

An organized way to convey a path of experience, wisdom, perfection, or acculturation.

Depicts an evolutionary progression of an attribute, characteristic, pattern, or practice.

The subject of a maturity model can be objects or things, ways of doing something, characteristics of something, practices, controls, or processes.
Maturity Models Provide...

Means for assessing and benchmarking performance
Ability to assess how a set of characteristics have evolved
Expression of body knowledge of best practices
Identification of gaps and improvement plans
Roadmap for model-based improvement
Demonstrated results of improvement efforts
Common language or taxonomy
Key Components of a Maturity Model

Levels
- The measurement scale
- The transitional states

Domains
- Logical groupings of like attributes into areas of importance to the subject matter and intent of the model
- Logical groupings of like practices, processes, or good things to do

Attributes
- Core content of the model arranged by domains and levels
- Typically based on observed practices, standards, or expert knowledge

Diagnostic Methods
- For assessment, measurement, gap identification, benchmarking

Improvement Roadmaps
- To guide improvement efforts (e.g., Plan-Do-Check-Act)
Types of Maturity Models

There are three types of maturity models

- Progression Maturity Models
- Capability Maturity Models (CMM)
- Hybrid Maturity Models

One or more may be appropriate for your particular needs

Not all maturity models are CMMs
Progression Maturity Models

Simple progression or scaling of an attribute, characteristic, pattern, or practice

Levels describe higher states of achievement, advancement, completeness, or evolution

Levels can be arbitrary as agreed upon by users, industry, etc.
Progression Maturity Models - Example

<table>
<thead>
<tr>
<th>A Maturity Progression for Toy Building Bricks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lego Mindstorms</td>
</tr>
<tr>
<td>Lego Architecture</td>
</tr>
<tr>
<td>Lego Technic</td>
</tr>
<tr>
<td>Lego City</td>
</tr>
<tr>
<td>Lego Duplo</td>
</tr>
</tbody>
</table>
Progression Maturity Models - Example

A Maturity Progression for Human Mobility

- Fly
- Sprint
- Run
- Jog
- Walk
- Crawl

A Maturity Progression for Authentication

- Three-factor authentication
- Two-factor authentication
- Addition of changing every 60 days
- Use of strong passwords
- Use of simple passwords

Progress does not necessarily equate to maturity
Progression Maturity Models - Example

Higher levels may be characterized as “tool-enabled”

Lower levels may be characterized as “primitive”

These characterizations are typically arbitrary

<table>
<thead>
<tr>
<th>A Maturity Progression for Counting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer</td>
</tr>
<tr>
<td>Calculator</td>
</tr>
<tr>
<td>Adding machine</td>
</tr>
<tr>
<td>Slide rule</td>
</tr>
<tr>
<td>Abacus</td>
</tr>
<tr>
<td>Pencil and paper</td>
</tr>
<tr>
<td>Sticks/Stones</td>
</tr>
<tr>
<td>Fingers</td>
</tr>
</tbody>
</table>
Progression Model Example: SGMM

Smart Grid Maturity Model

175 Characteristics: Features you would expect to see at each stage of the smart grid journey
Benefits and Limitations of Progression Models

**Benefits**

- Provides a transformative roadmap
- Simple to understand and adopt; low adoption cost
- Easy to recalibrate as technologies and practices advance

**Limitations**

- Levels are arbitrarily defined and may be meaningless
- Achieving higher levels does not necessarily translate into “maturity”
- Often confused with CMMs—thus users inaccurately project traits of CMMs on progression models
Capability Maturity Models (CMM)

A more complex instrument

Characterizes

- the maturity of processes
- the degree to which processes are institutionalized
- the degree to which the organization demonstrates process maturity
- the maturity of the culture of the organization

Levels reflect the degree to which a particular set of practices have been institutionalized

- Institutionalized processes are more likely to be retained during times of stress.
What do these organizations have in common?

Customer Happiness

Customer Service

Strong Culture

Chain of Command
Unit Cohesion
Regulations

Tradition
Protection
CMM Levels – An Example

Processes are acculturated, defined, measured, and governed

Practices are performed

Practices are incomplete

Level 3
- Defined

Level 2
- Managed

Level 1
- Performed

Level 0
- Incomplete

Higher degrees of institutionalization translate to more stable processes that

• are repeatable
• produce consistent results over time
• are retained during times of stress
### CMM Levels – Another Example

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optimized</td>
<td>Continuous and effective, integrated, proactive, usually automated</td>
</tr>
<tr>
<td>Measured</td>
<td>Well-managed, formal, often automated, evaluated frequently</td>
</tr>
<tr>
<td>Defined</td>
<td>Intuitive, not documented, occurs only when necessary</td>
</tr>
<tr>
<td>Repeatable</td>
<td>Intuitive, not documented, occurs only when necessary</td>
</tr>
<tr>
<td>Ad hoc</td>
<td>Occasional, not consistent, not planned, disorganized</td>
</tr>
<tr>
<td>Nonexistent</td>
<td>Not understood, not formalized, need is not recognized</td>
</tr>
</tbody>
</table>
## Examples of CMM Levels

<table>
<thead>
<tr>
<th>Example 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optimized</td>
</tr>
<tr>
<td>Quantitatively Managed</td>
</tr>
<tr>
<td>Defined</td>
</tr>
<tr>
<td>Managed</td>
</tr>
<tr>
<td>Ad hoc</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Example 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Externally integrated</td>
</tr>
<tr>
<td>Internally integrated</td>
</tr>
<tr>
<td>Managed</td>
</tr>
<tr>
<td>Performed</td>
</tr>
<tr>
<td>Initiated</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Example 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared</td>
</tr>
<tr>
<td>Defined</td>
</tr>
<tr>
<td>Measured</td>
</tr>
<tr>
<td>Managed</td>
</tr>
<tr>
<td>Planned</td>
</tr>
<tr>
<td>Performed but ad hoc</td>
</tr>
<tr>
<td>Incomplete</td>
</tr>
</tbody>
</table>
Capability Maturity Model Example: CERT-RMM

Framework for managing and improving operational resilience

http://www.cert.org/resilience/

“...an extensive super-set of the things an organization could do to be more resilient.”

- CERT-RMM adopter
CMM Example: CERT-RMM

### CERT-RMM Process Areas (Domains)

<table>
<thead>
<tr>
<th>Access Management</th>
<th>Measurement and Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Definition and Mgmt.</td>
<td>Monitoring</td>
</tr>
<tr>
<td>Communications</td>
<td>Organizational Process Focus</td>
</tr>
<tr>
<td>Compliance</td>
<td>Organizational Process Definition</td>
</tr>
<tr>
<td>Controls Management</td>
<td>Organizational Training &amp; Awareness</td>
</tr>
<tr>
<td>Enterprise Focus</td>
<td>People Management</td>
</tr>
<tr>
<td>Environmental Control</td>
<td>Resilience Requirements Development</td>
</tr>
<tr>
<td>External Dependencies</td>
<td>Resilience Requirements Mgmt.</td>
</tr>
<tr>
<td>Human Resource Management</td>
<td>Risk Management</td>
</tr>
<tr>
<td>Identity Management</td>
<td>Service Continuity</td>
</tr>
<tr>
<td>Incident Management &amp; Control</td>
<td>Technology Management</td>
</tr>
<tr>
<td>Knowledge &amp; Information Mgmt.</td>
<td>Vulnerability Analysis &amp; Resolution</td>
</tr>
</tbody>
</table>

© 2013 Carnegie Mellon University
Consider the **Incident Management and Control (IMC)** domain from CERT-RMM:

- **Goal 1**: Establish the IMC process
- **Goal 2**: Detect events
- **Goal 3**: Declare incidents
- **Goal 4**: Respond to and recover from incidents
- **Goal 5**: Establish incident learning
CMM Example: CERT-RMM

Level 0
Incomplete
“We don’t do (all of) the practices.”

Level 1
Performed
“We do the practices.”

Level 2
Managed
“We do the practices AND we plan and govern the process, resource it, train people to do it, monitor it, etc…”

Level 3
Defined
We do everything in level 2 AND we have a defined process and collect improvement information.”

Institutionalization is cumulative
## Benefits and Limitations of CMMs

### Benefits

- Provides for measurement of core competencies
- Provides for rigorous measurement of capability—the ability to retain core competencies under times of stress
- Can provide a path to quantitative measurement

### Limitations

- Sometimes difficult to understand and apply; high adoption cost
- “Maturity” may not translate into actual results
- Potential false sense of achievement: achieving high maturity in security practices may not mean the organization is “secure”
Compare: Progression vs CMM

**Progression Model**
- **Level 3**
  - Run
- **Level 2**
  - Jog
- **Level 1**
  - Walk
- **Level 0**
  - Crawl

**Capability Model**
- **Level 3**
  - Defined
- **Level 2**
  - Managed
- **Level 1**
  - Performed
- **Level 0**
  - Incomplete

Distribuion of core practices across levels

Distribuion of institutionalizing features

Core practices
Hybrid Maturity Model

Combines the best features of progression and capability maturity models

- Allows for measurement of evolution or achievement as in progression models
- Adds the ability to measure capability or institutionalization with the rigor of a CMM

Levels reflect both achievement and capability

Transitions between levels:

- Similar to a capability model (i.e., describe capability maturity)
- Architecturally use the characteristics, indicators, attributes, or patterns of a progression model
Hybrid Maturity Models

<table>
<thead>
<tr>
<th>Domain 1</th>
<th>Domain 2</th>
<th>Domain n</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Measured</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Managed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Planned</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level 0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incomplete</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Domains: Specific categories of attributes, characteristics, patterns, or practices that form the content of the model.

Model content: Specific attributes, characteristics, patterns, or practices that represent *progression and capability*.

Maturity levels: Defined sets of characteristics and outcomes, *plus capability considerations*.
### Hybrid Model Example: ES-C2M2

<table>
<thead>
<tr>
<th>Maturity Indicator Levels</th>
<th>0 Not Performed</th>
<th>1 Initiated</th>
<th>2 Performed</th>
<th>3 Managed</th>
<th>X Reserved</th>
</tr>
</thead>
</table>

- **1 Maturity Indicator Level**: Reserved for future use
- **4 Maturity Indicator Levels**: Defined progressions of practices
- **Each cell contains the defining practices for the domain at that maturity indicator level**

### 10 Model Domains: Logical groupings of cybersecurity practices

- RISK
- ASSET
- ACCESS
- THREAT
- SITUATION
- SHARING
- RESPONSE
- DEPENDENCIES
- WORKFORCE
- CYBER

---

**Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)**
## Benefits and Limitations of Hybrid Models

**Benefits**

- Provides for easy measurement of core competencies as well as approximation of capability
- Can adapt easily to evolution of technologies and practices without sacrificing capability measurement
- Low adoption cost

**Limitations**

- “Maturity” concept is approximated; not as rigorous as CMM
- Combination of attributes with institutionalizing features at each level can be arbitrary
Closing Thoughts

- A few cautions
- Determining when and which type to use
First and Foremost

Have a clear understanding of your business objectives for using any type of improvement model

- How the model will meet these objectives

Understand how this initiative fits with others that are mainstream for the organization (not a new add-on)

Have visible sponsorship of executives and senior leaders who are essential for success

Have well-defined outcome measures that are regularly reported and reviewed

Have a plan and committed resources
A Few Cautions

Progression models may be easier to adopt but may not be sustainable (aka sticky)

Definitions of levels can be arbitrary

Measuring process performance and maturity is useful but may not be sufficient

Exercise care when using maturity models for specific purposes
Progression Models May Not Be Sustainable

A progression model provides a roadmap or scale of a particular characteristic, indicator, attribute, pattern, or practice

- Focuses on practices or controls and their progression from least mature to most mature
- Cannot be used to measure the extent to which an organization is capable of sustaining the practice in times of disruption and stress (the practice has not become part of the DNA)

A hybrid or capability maturity model adds the dimension of organizational capability to practice progression

- Thus able to measure an organization’s “resilience” in the presence of disruption and stress
Definitions of Levels Can Be Arbitrary

Often defined by consensus of subject matter experts

Can simply reflect a plateau or a place in a progression or scale

Often have not been validated or are difficult to validate based on experience and measurement

May neglect to represent the capability and capacity of an organization to sustain operations in the presence of disruption and stress
Measuring Process Performance May Not Be Sufficient

Experience demonstrates that the quality of the process directly affects the quality of the product

- However, process performance and maturity are only one aspect

Also need to consider the performance and maturity of

- The product and its outcomes
- The supporting technologies
- The environment within which the product operates
- Knowledge, skills, and abilities of people with respect to all of these
- Which of these dimensions to emphasize given product objectives
When Does It Make Sense to Use Maturity Models?

Requirement for a structured approach

Demonstrated, measurable results based on an established body of knowledge

A defined roadmap from a current state to a desired state

An ability to monitor and measure progress, particularly in the presence of change

• Response to a strategic improvement or new product/new market objective
When Does It Make Sense to Use Maturity Models? (cont.)

Desire to answer these questions in a repeatable, predictable manner:

- How do I compare with my peers? (ability to benchmark)
- How can I determine how secure I am and if I am secure enough?
- How do I measure my current state? Characterize my desired state?
- What concrete actions do I need to take to improve? And in what order?
- How do I measure progress toward my desired state?
- How do I adapt to change?
Exercise Care When Using Maturity Models

If the immediate need is to respond to an in-progress disruptive event

- Robust processes are not yet in place
- Current protection and defensive mechanisms are failing
- Need to stop the bleeding, stabilize operations, rely on experts

In response to current and new compliance requirements

- In a highly regulated industry
- Must demonstrate compliance with specific laws, regulations and standard(s)
- Standard, defined processes and mapping new compliance requirements to these can be quite effective
References


As projects continue to grow in scale and complexity, effective collaboration across geographical, cultural, and technical boundaries is increasingly prevalent and essential to system success. SATURN 2012 will explore the theme of “Architecture: Catalyst for Collaboration.”

Introduction to the CERT Resilience Management Model
February 18 - 20, 2014 (SEI, Arlington, VA)
June 17 - 19, 2014 (SEI, Pittsburgh, PA)
See Materials Widget for course document