RSACONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Buyer Beware: How To Be a Better Consumer of Security Maturity Models

SESSION ID: GRC-R01

Julia Allen

Software Engineering Institute
Carnegie Mellon University
jha@sei.cmu.edu

Nader Mehravari

Software Engineering Institute
Carnegie Mellon University
nmehravari@sei.cmu.edu

Objectives

Maturity models are effective tools for improving an organization’s security capabilities and outcomes. But knowing which model to use and how to use it is paramount to success.

- Improve your understanding of important maturity model concepts
- Learn about the use of maturity models by examining recent examples in the cybersecurity and resilience domains
- Be aware of caution flags when dealing with maturity models
- Determine how to choose the right model for your specific needs (improvement vs. assessment etc..)

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?
- **Background and History**
  - Where do maturity models come from?
  - Early development and instantiation
- **ABCs of Maturity Models**
  - What are maturity models?
  - Types of maturity models
  - Real life examples
- **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.

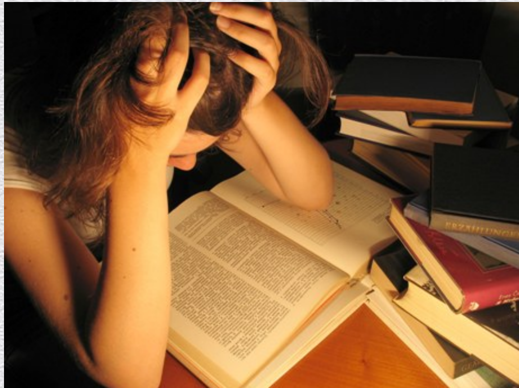
Challenges at Hand

How can you tell if you are doing a good job of managing these changes?

What are effective ways to monitor your progress?

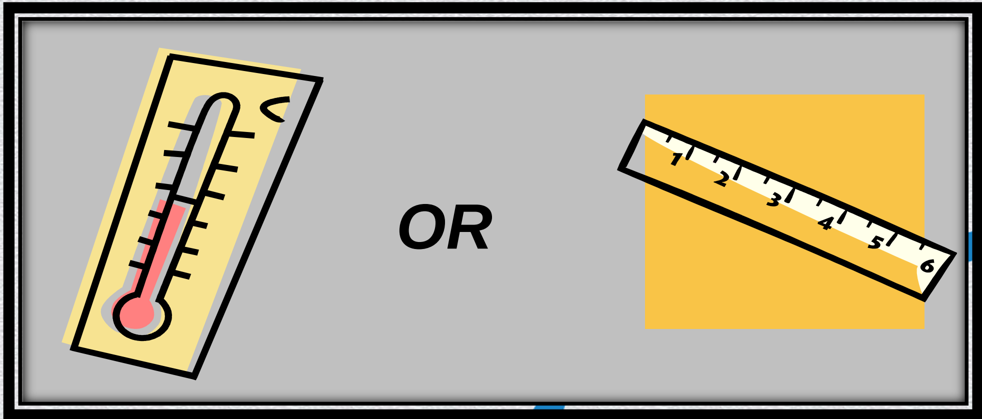
How do you manage the interactions of systems and processes that are continually changing?

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**?



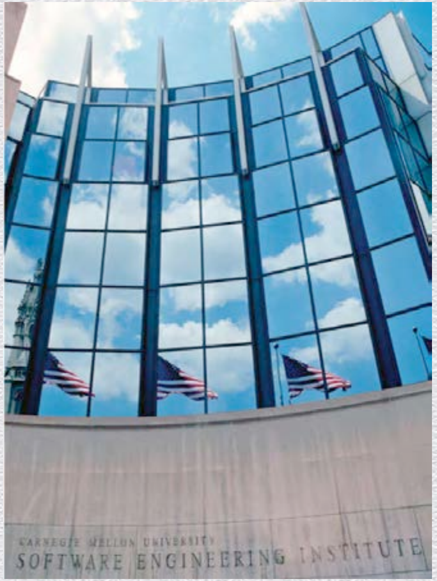
Observation

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

CERT | Software Engineering Institute | Carnegie Mellon



Carnegie Mellon University

Software Engineering Institute (SEI)

- Federally funded research and development center
- Basic and applied research in partnership with government and private organizations
- Helps organizations improve development, operation, and management of software-intensive and networked systems

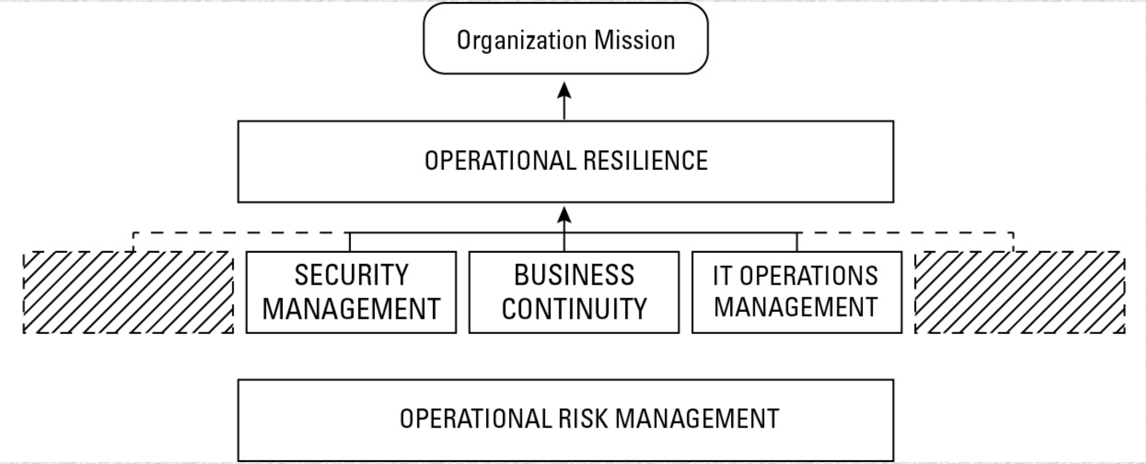
CERT – *Anticipating and solving our nation's cybersecurity challenges*

- Largest technical program at the SEI
- Focused on internet security, digital investigation, secure systems, insider threat, operational resilience, vulnerability analysis, network situational awareness, and coordinated response

CMU-SEI-CERT Cyber Risk Management Team

Engaged in applied research, education and training, putting improvements into practice, and enabling our federal, state, and commercial partners

In areas dealing with operational resilience, resilience management, operational risk management, and integration of cybersecurity, business continuity, disaster recovery, and IT operations

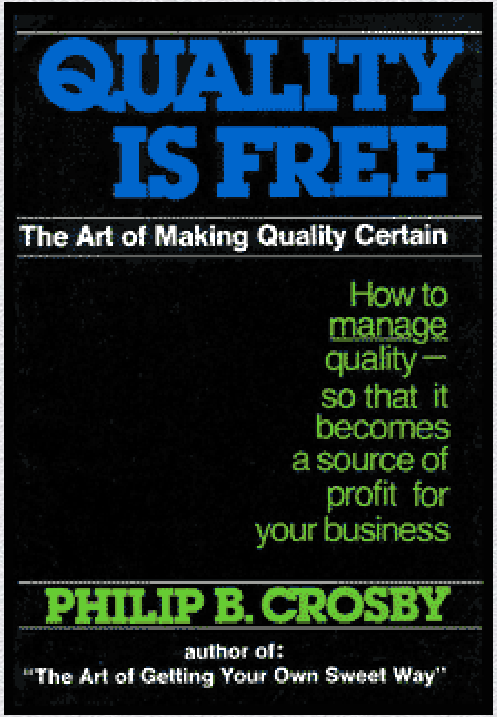


http://www.cert.org/resilience/

Background and History

- Where do maturity models come from?
- Early development and instantiation

In the beginning there was “Quality is Free”



QUALITY IS FREE

The Art of Making Quality Certain

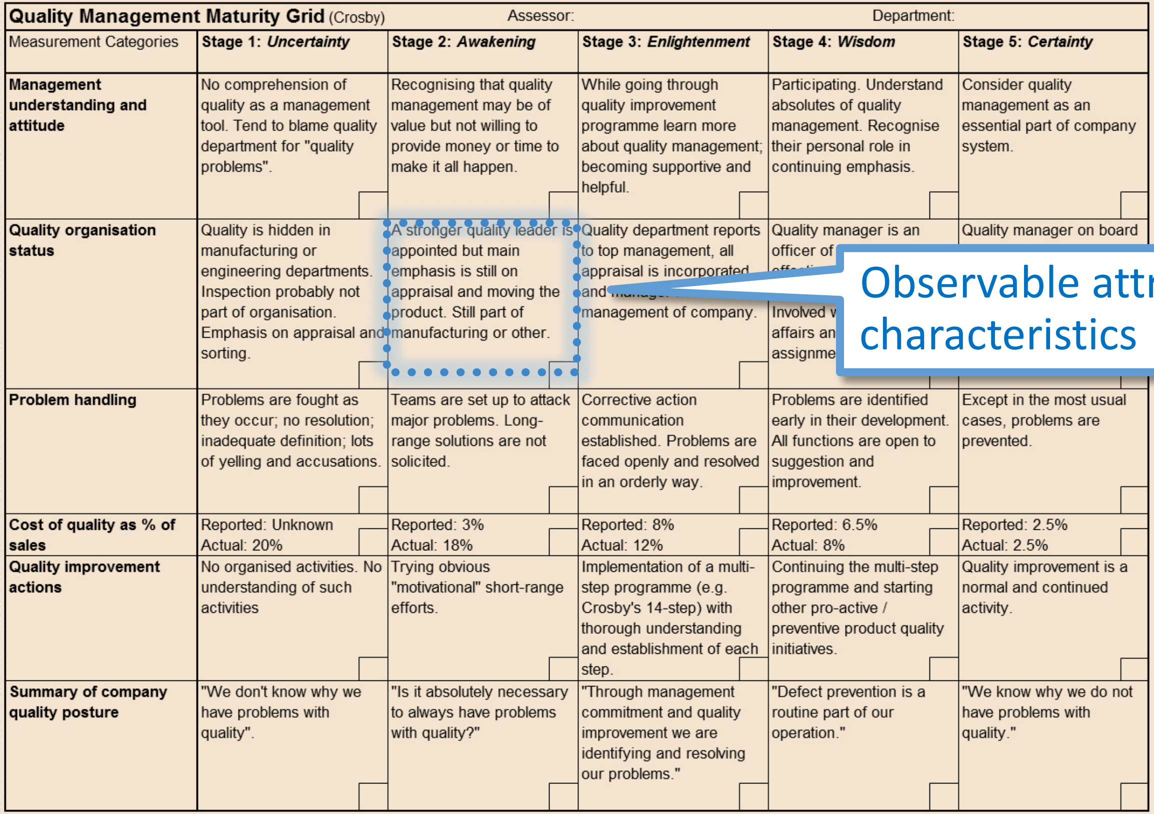
How to manage quality — so that it becomes a source of profit for your business

PHILIP B. CROSBY

author of:
“The Art of Getting Your Own Sweet Way”

- Viewed “quality” as a characteristic owned by everyone in the organization
- Created the Quality Management Maturity Grid to express organizational maturity across a range of quality attributes or categories
- Defined observable outcomes as benchmarks

The Quality Management Maturity Grid



Quality Management Maturity Grid (Crosby) Assessor: Department:

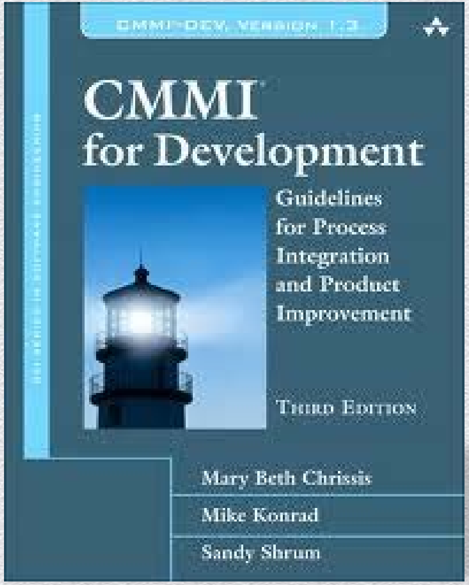
Measurement Categories	**Stage 1:** ***Uncertainty***	**Stage 2:** ***Awakening***	**Stage 3:** ***Enlightenment***	**Stage 4:** ***Wisdom***	**Stage 5:** ***Certainty***
Management understanding and attitude	No comprehension of quality as a management tool. Tend to blame quality department for "quality problems".	Recognising that quality management may be of value but not willing to provide money or time to make it all happen.	While going through quality improvement programme learn more about quality management; becoming supportive and helpful.	Participating. Understand absolutes of quality management. Recognise their personal role in continuing emphasis.	Consider quality management as an essential part of company system.
Quality organisation status	Quality is hidden in manufacturing or engineering departments. Inspection probably not part of organisation. Emphasis on appraisal and sorting.	A stronger quality leader is appointed but main emphasis is still on appraisal and moving the product. Still part of manufacturing or other.	Quality department reports to top management, all appraisal is incorporated and manage management of company.	Quality manager is an officer of Involved w affairs an assignme	Quality manager on board
Problem handling	Problems are fought as they occur; no resolution; inadequate definition; lots of yelling and accusations.	Teams are set up to attack major problems. Long-range solutions are not solicited.	Corrective action communication established. Problems are faced openly and resolved in an orderly way.	Problems are identified early in their development. All functions are open to suggestion and improvement.	Except in the most usual cases, problems are prevented.
Cost of quality as % of sales	Reported: Unknown Actual: 20%	Reported: 3% Actual: 18%	Reported: 8% Actual: 12%	Reported: 6.5% Actual: 8%	Reported: 2.5% Actual: 2.5%
Quality improvement actions	No organised activities. No understanding of such activities	Trying obvious "motivational" short-range efforts.	Implementation of a multi-step programme (e.g. Crosby's 14-step) with thorough understanding and establishment of each step.	Continuing the multi-step programme and starting other pro-active / preventive product quality initiatives.	Quality improvement is a normal and continued activity.
Summary of company quality posture	"We don't know why we have problems with quality".	"Is it absolutely necessary to always have problems with quality?"	"Through management commitment and quality improvement we are identifying and resolving our problems."	"Defect prevention is a routine part of our operation."	"We know why we do not have problems with quality."

Observable attributes or characteristics

#RSAC

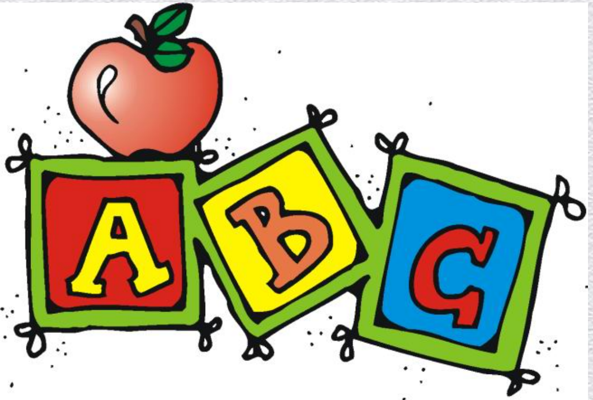
Evolution of the QMMG

- 1986 – Watts Humphrey formalizes the Process Maturity Framework into the Capability Maturity Model for Software (SW-CMM) at Carnegie Mellon’s Software Engineering Institute
- Driven by USAF need to *measure capabilities* of software contractors
- Architecturally based on the QMMG but reflective of observed best practices for software development
- 2000 - CMM Integration (CMMI) created to combine software, systems engineering and integrated product processes; now at v1.3



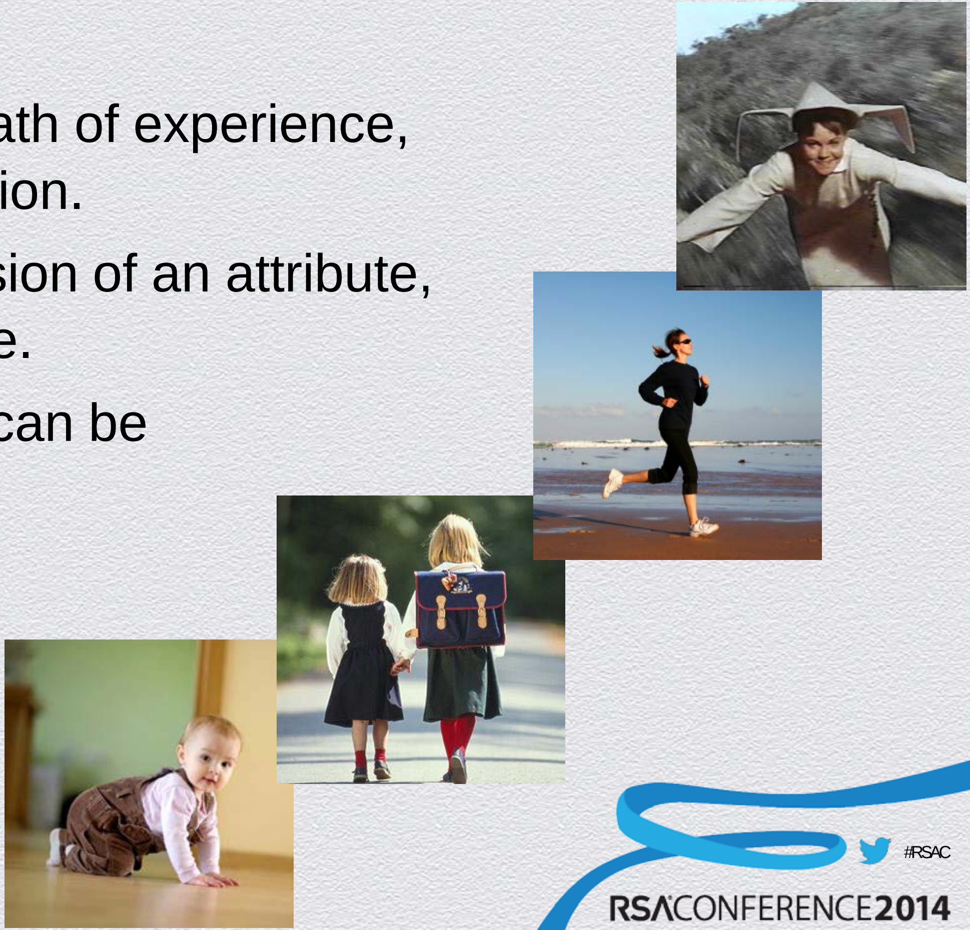
ABCs of Maturity Models

- What are maturity models?
- Types of maturity models
- Examples of maturity models



Maturity Model Defined

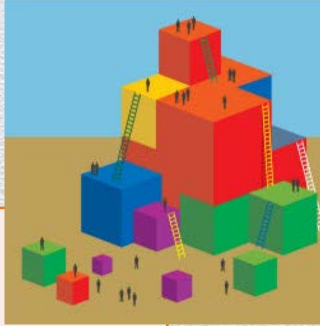
- An organized way to convey a path of experience, wisdom, perfection, or acculturation.
- Depicts an evolutionary progression of an attribute, characteristic, pattern, or practice.
- The subject of a maturity model can be objects or things, ways of doing something, characteristics of something, practices, controls, or processes.



Maturity Models Provide…

- Means for assessing and benchmarking performance
- Ability to assess how a set of characteristics have evolved
- Expression of a body of knowledge of best practices
- Means to identify gaps and develop 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 (Plan-Do-Check-Act; Observe-Orient-Decide-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

Smart Grid Maturity Model

ELECTRICITY SUBSECTOR CYBERSECURITY CAPABILITY MATURITY MODEL (ES-C2M2)

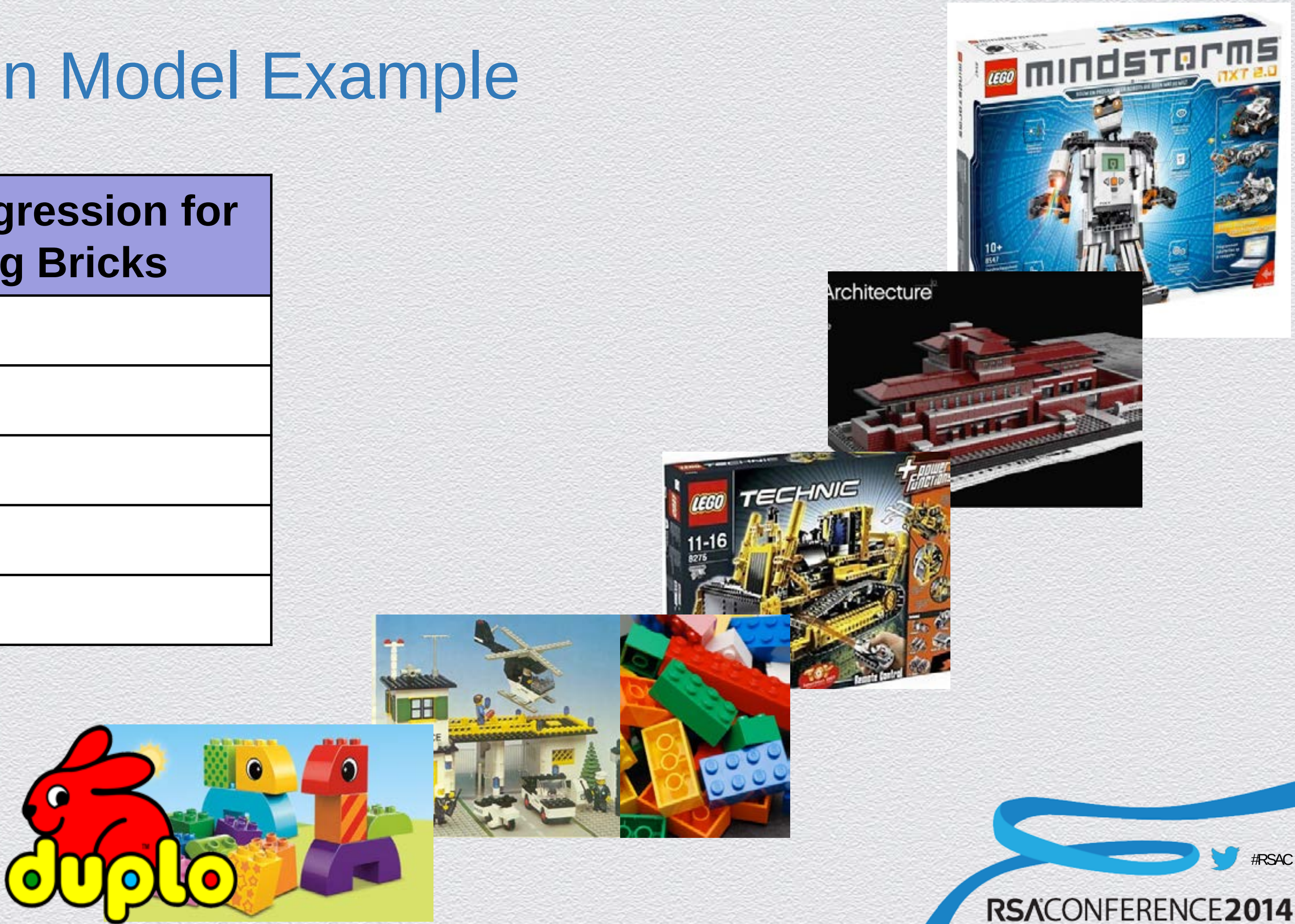
Version 1.0
31 May 2012

Progression Model Example

- 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 Model Example

A Maturity Progression for Toy Building Bricks
Lego Mindstorms
Lego Architecture
Lego Technic
Lego City
Lego Duplo



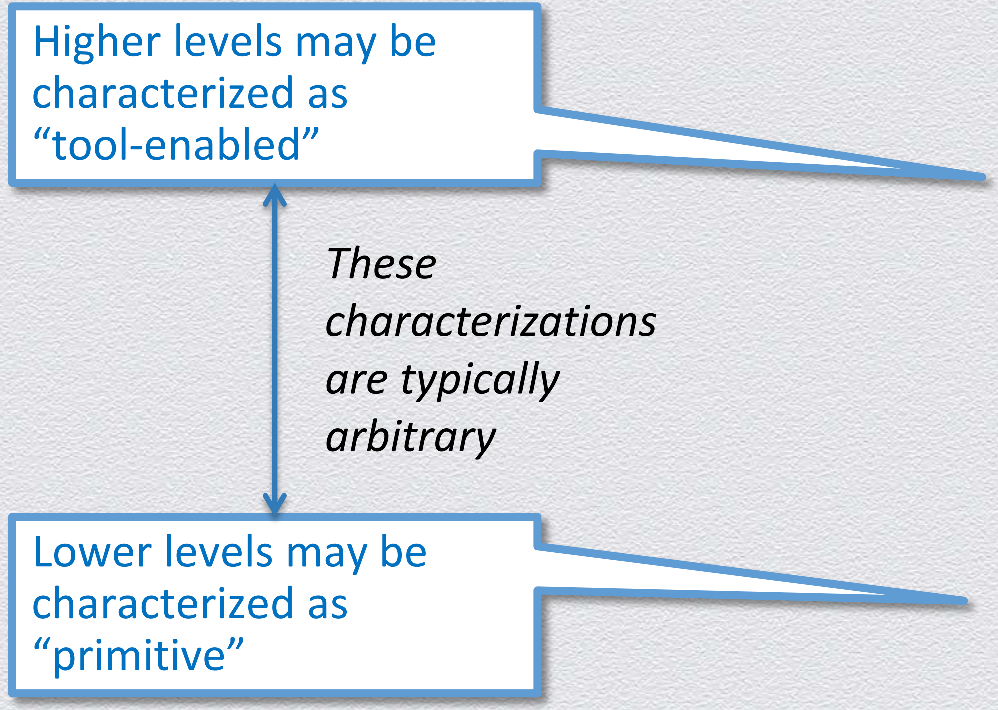
Progression Model Examples

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 equal maturity

Progression Model Cyber Example



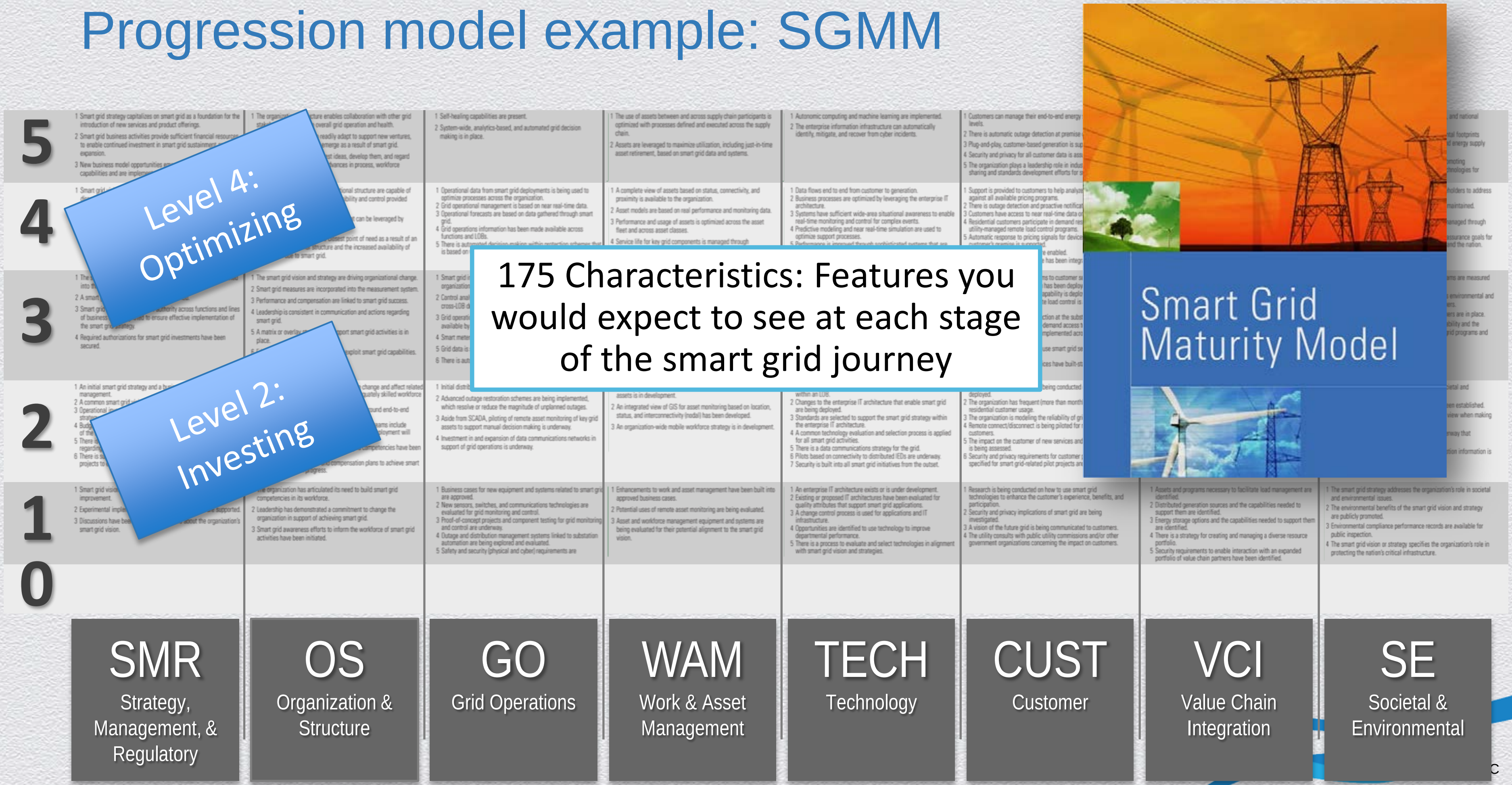
Higher levels may be characterized as "tool-enabled"

These characterizations are typically arbitrary

Lower levels may be characterized as "primitive"

A Maturity Progression for Counting
Computer
Calculator
Adding machine
Slide rule
Abacus
Pencil and paper
Sticks/Stones
Fingers

Progression model example: SGMM



175 Characteristics: Features you would expect to see at each stage of the smart grid journey

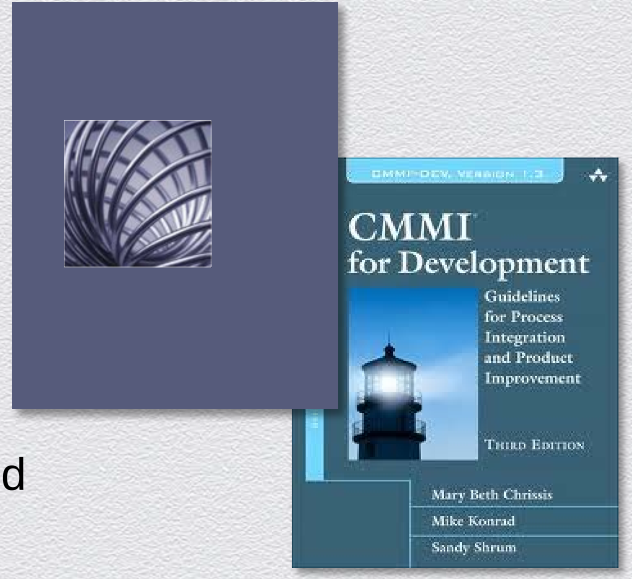
SMR	OS	GO	WAM	TECH	CUST	VCI	SE
Strategy, Management, & Regulatory	Organization & Structure	Grid Operations	Work & Asset Management	Technology	Customer	Value Chain Integration	Societal & Environmental

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 for achieving objectives
  - 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 maturity of the culture of the organization
  - the extent to which the organization demonstrates process maturity
- Levels reflect the extent 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

Chain of Command
Unit Cohesion

Strong Culture

Customer Service

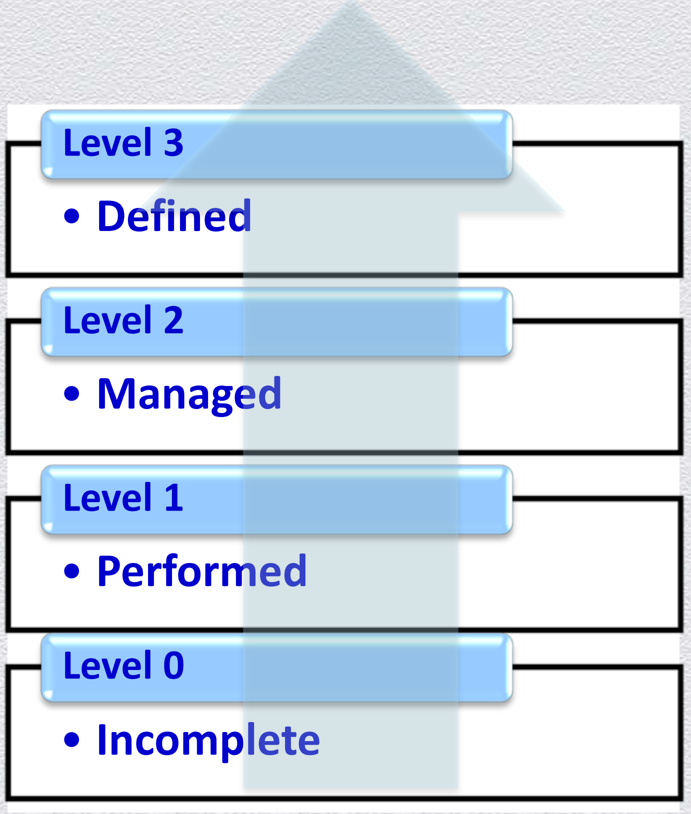
Tradition
Protection

Capability Maturity Model Levels

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*

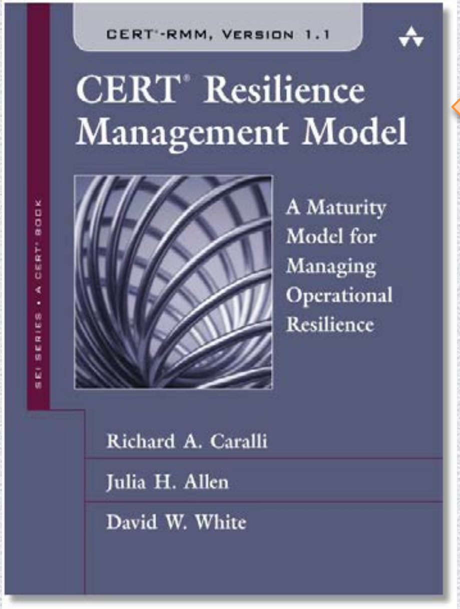
Examples of CMM Levels

Example 1
Optimized
Quantitatively Managed
Defined
Managed
Ad hoc

Example 2
Externally integrated
Internally integrated
Managed
Performed
Initiated

Example 3
Shared
Defined
Measured
Managed
Planned
Performed but ad hoc
Incomplete

Capability Maturity Model Example: CERT-RMM *(1 of 6)*



CERT®-RMM, Version 1.1

CERT® Resilience Management Model

A Maturity Model for Managing Operational Resilience

SEI Series • A CERT® Book

Richard A. Caralli

Julia H. Allen

David W. White

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

Framework for managing and improving operational resilience

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

- CERT-RMM adopter

CERT-RMM *(2 of 6)*

- Operational Resilience Perspective

  The **emergent** property of an entity that can continue to carry out its mission in the presence of operational stress and disruption that does not exceed its limit

- Disruptions come from realized risk
  - Natural or manmade
  - Accidental or intentional
  - Small or large
  - Information technology or not
  - Cyber or kinetic

CERT-RMM *(3 of 6)*

- Security and business continuity are risk management processes
- For operational risk management to be effective, these activities must work toward the same goals
- Operational resilience emerges from effective operational risk management

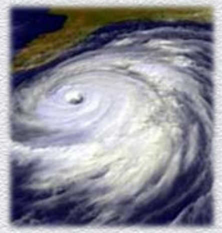
Actions of people

```
A fatal exception
000059F8. The curr

* Press any key to
* Press CTRL+ALT+D
  lose any unsaved
```

Systems and technology failures

Failed internal processes



External events

CERT-RMM *(4 of 6)*

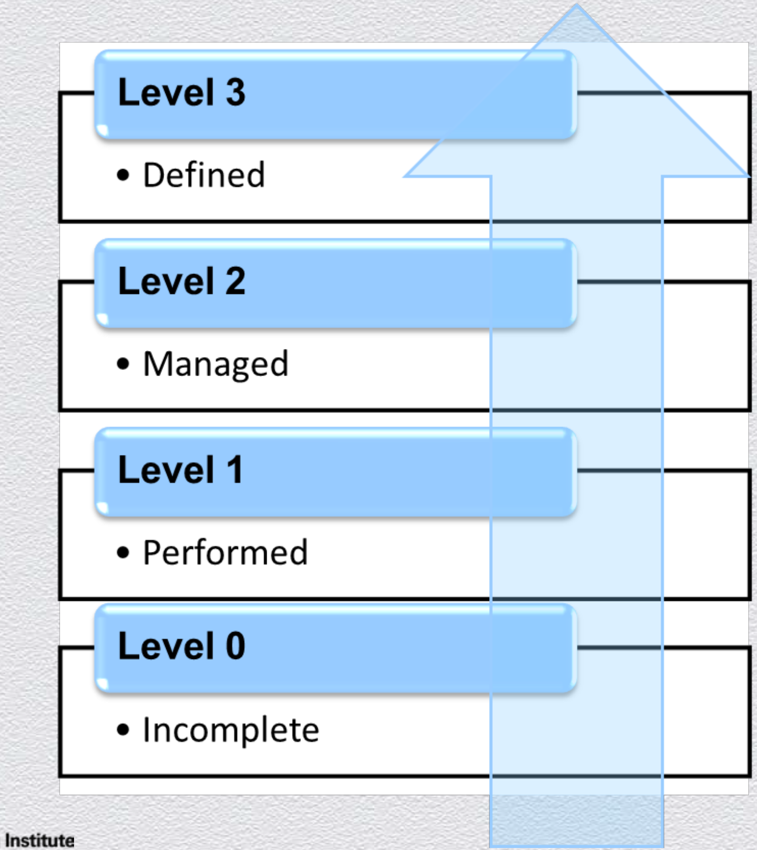
- Most comprehensive framework for managing and improving operational resilience
- Guides implementation and management of operational resilience activities
- Enables and promotes the **convergence** of
  - COOP, IT Disaster Recovery, Business Continuity
  - Information Security, Cybersecurity
  - IT Operations

CERT-RMM Process Areas (Domains) *(5 of 6)*

- Access Management
- Asset Definition and Management
- Communications
- Compliance
- Controls Management
- Enterprise Focus
- Environmental Control
- External Dependencies Management
- Financial Resource Management
- Human Resource Management
- Identity Management
- Incident Management & Control
- Knowledge & Information Management

- Measurement and Analysis
- Monitoring
- Organizational Process Definition
- Organizational Process Focus
- Organizational Training & Awareness
- People Management
- Resilience Requirements Development
- Resilience Requirements Management
- Resilient Technical Solution Engineering
- Risk Management
- Service Continuity
- Technology Management
- Vulnerability Analysis & Resolution

CERT-RMM Capability Levels *(6 of 6)*



Level 3

- Defined

Level 2

- Managed

Level 1

- Performed

Level 0

- Incomplete

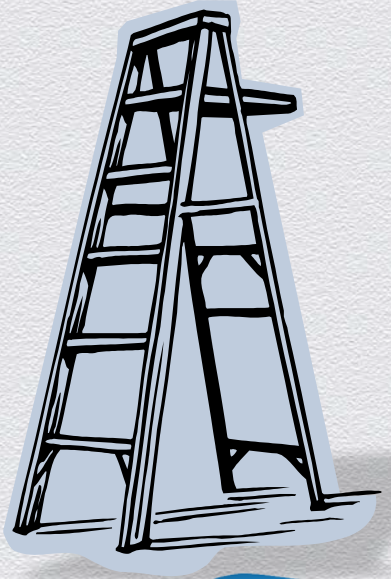
Processes are acculturated, defined, measured, and governed

Practices are performed

Incident Management & Control: An Example

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*



Incident Management by the CMM levels

Level 0

Incomplete

"We do *some* of the IMC practices."

Level 1

Performed

"We do *all* of the IMC practices."

Level 2

Managed

"We do the IMC 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

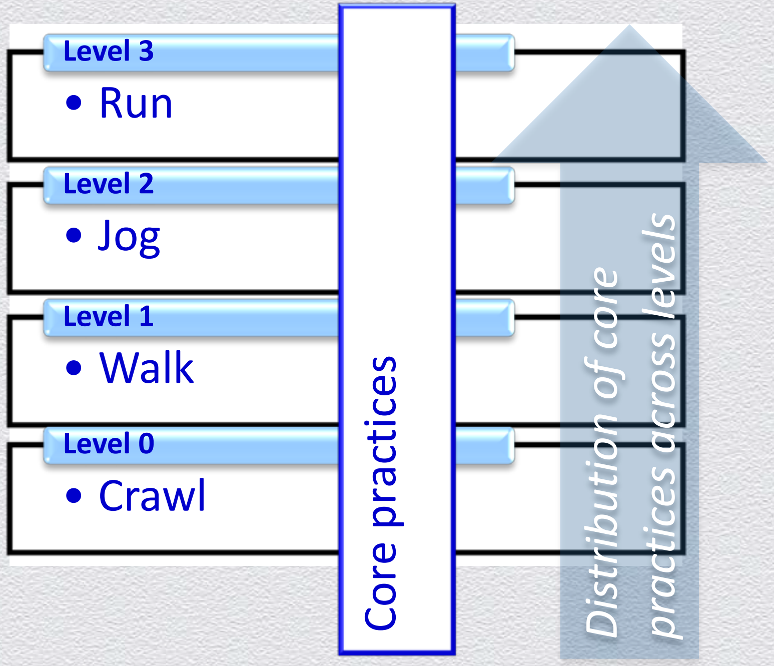
Benefits

- 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



Level 3
- Run

Level 2
- Jog

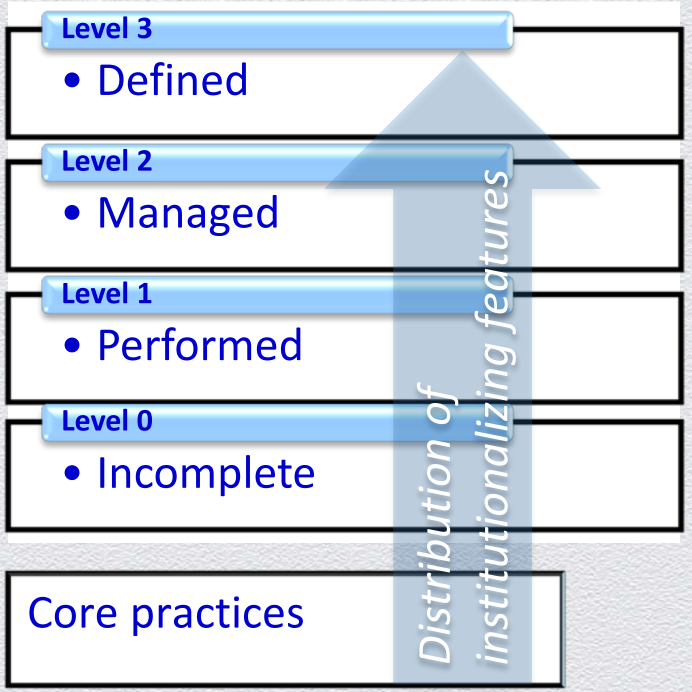
Level 1
- Walk

Level 0
- Crawl

Core practices

Distribution of core practices across levels

Progression Model



Level 3
- Defined

Level 2
- Managed

Level 1
- Performed

Level 0
- Incomplete

Core practices

Distribution of institutionalizing features

Capability Model

Hybrid Models

- Combine best features of progression and capability maturity models
  - Allow for measurement of evolution or achievement as in progression models
  - Add 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 Model

Capability or "maturity" levels

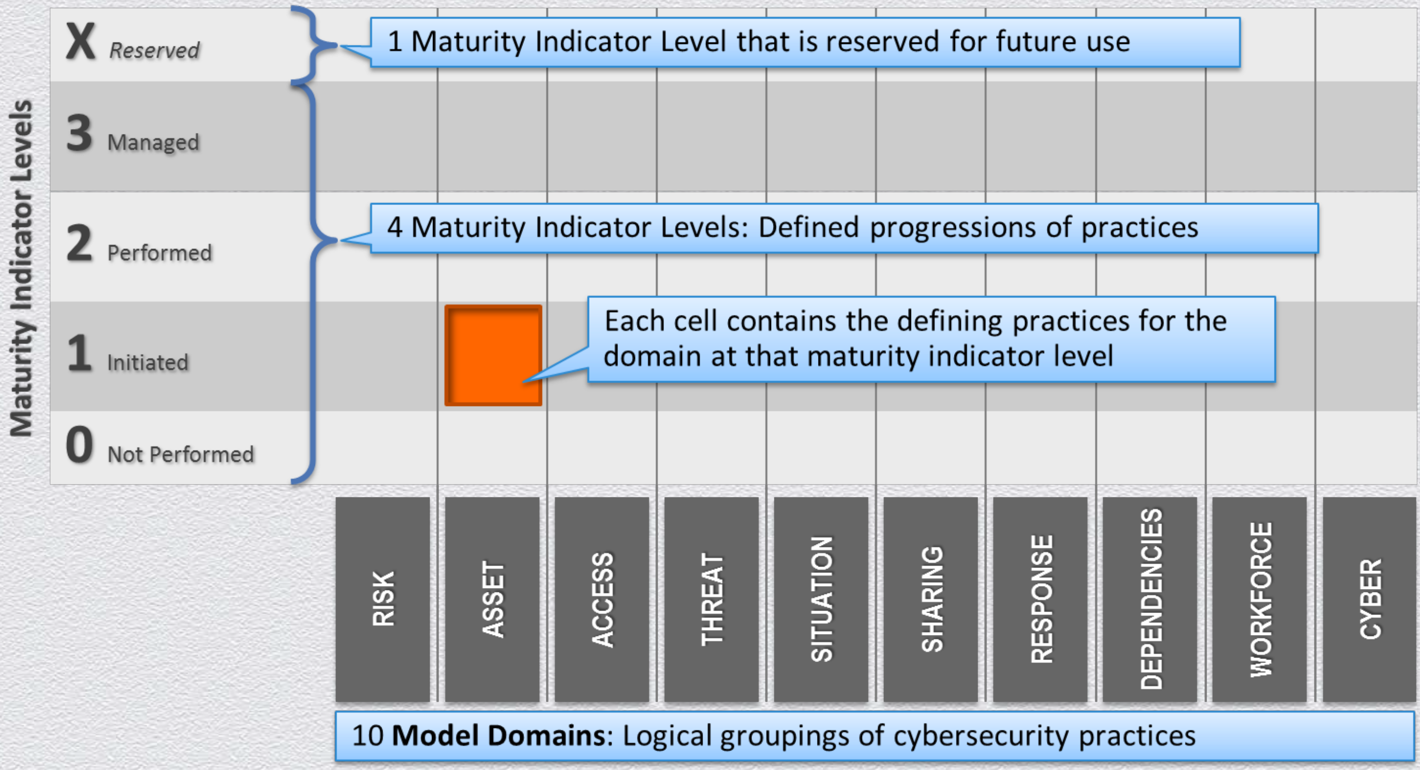
	Domain 1	Domain 2	Do		
Level 4 *Defined*					
Level 3 *Measured*					
Level 2 *Managed*					
Level 1 *Planned*					
Level 0 *Incomplete*					

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



Maturity Indicator Levels

X *Reserved*

3 Managed

2 Performed

1 Initiated

0 Not Performed

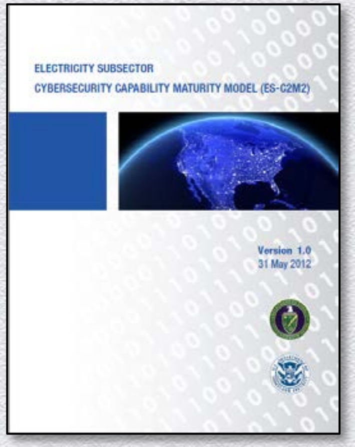
1 Maturity Indicator Level that is reserved for future use

4 Maturity Indicator Levels: Defined progressions of practices

Each cell contains the defining practices for the domain at that maturity indicator level

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

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



ELECTRICITY SUBSECTOR
CYBERSECURITY CAPABILITY MATURITY MODEL (ES-C2M2)

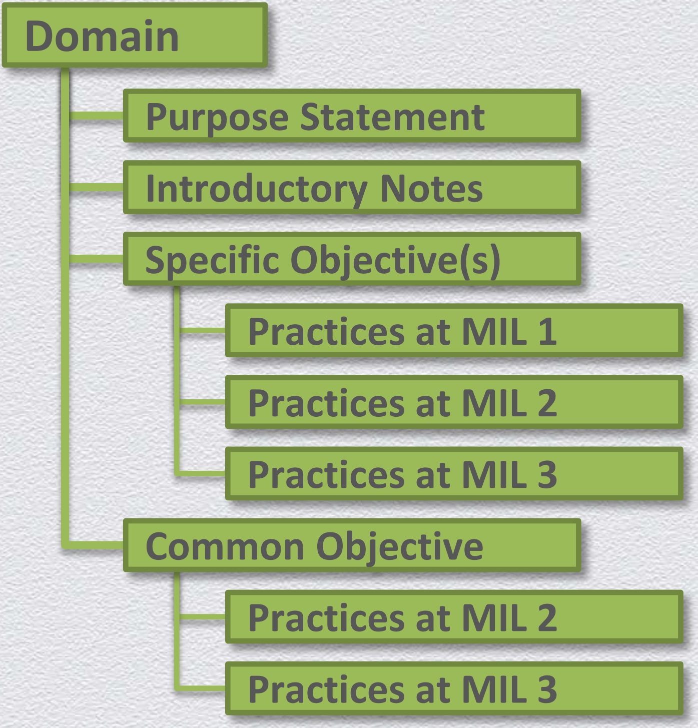
Version 1.0
31 May 2012

Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)

Hybrid Model Example: ES-C2M2 *(cont.)*

Level	Name	Description
MIL0	Not Performed	• MIL1 has not been achieved in the domain
MIL1	Initiated	• Initial practices are performed, but may be ad hoc
MIL2	Performed	• 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	• 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

Hybrid Model Example: ES-C2M2 *(cont.)*



Domain

Purpose Statement

Introductory Notes

Specific Objective(s)

Practices at MIL 1

Practices at MIL 2

Practices at MIL 3

Common Objective

Practices at MIL 2

Practices at MIL 3

Intent and overview

One or more progressions of practices that are unique to the domain

Progression of practices that describe institutionalization activities – same in each domain

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

Thank you for your attention…

CERT-RMM Contacts

Julia Allen
jha@sei.cmu.edu

Nader Mehravari
nmehravari@sei.cmu.edu

Lisa Young
lry@cert.org

Rich Caralli
rcaralli@cert.org

Richard Lynch
Public Relations — All Media Inquiries
public-relations@sei.cmu.edu

Pamela Curtis
pdc@cert.org

Joe McLeod
For info on working with us
jmcleod@sei.cmu.edu

SEI Customer Relations
customer-relations@sei.cmu.edu
412-268-5800

www.cert.org/resilience

Notices

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.

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.

DM-0000853