CERT® Resilience Management Model

A Maturity Model Approach to Managing Operational Resilience

SEI Webinar Series
28 July 2010

Rich Caralli
Technical Manager – CERT Resilient Enterprise Management Team
# CERT Resilience Management Model: A Maturity Model Approach to Managing Operational Resilience

**Report Type:**

- 00-00-2010 to 00-00-2010

**Performing Organization:**

Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, 15213

**Distribution/Availability Statement:**

Approved for public release; distribution unlimited

**Subject Terms:**

- unclassified
- unclassified
- unclassified

**Limitation of Abstract:**

Same as Report (SAR)

**Number of Pages:**

76
Introduction

Rich Caralli

Technical Manager – CERT Resilient Enterprise Management Team

25+ years in IT Audit and IT Management in financial services, manufacturing, and energy

8 years @ SEI concentrating in information security risk management

BS-Accounting; MBA

Frequent lecturer in Carnegie Mellon Heinz School and CIO Institute
Agenda

What is CERT-RMM?

History

Model Building Blocks

Model Architecture

The Capability Dimension

Determining Capability

CERT-RMM Credentialing

CERT-RMM and PS-Prep

CERT-RMM Product Suite
The **CERT® Resilience Management Model (CERT-RMM)** is a capability model for managing and improving operational resilience.

- Positions **operational resilience** in a process improvement view
- Includes 26 “**process areas**”
- Focuses on the operations phase of the lifecycle
- Defines “maturity” through “capability levels” consistent with CMMI
- Uses CMMI architecture for ease of adoption
- Includes a “continuous representation” for agile adoption
Distinguishing features of CERT®-RMM

CERT-RMM brings several innovative and advantageous concepts to the management of operational resilience.

- **The convergence advantage:** merging the disciplines of security, BC/DR, and IT ops into a single model
- **The process advantage:** elevating these disciplines to a process view, useful as an integration and measurement framework
- **The maturity advantage:** provides a foundation for practical institutionalization of practices—critical for retaining these practices under times of stress
History of CERT-RMM

How we got to CERT-RMM version 1.0
CERT-RMM background

CERT-RMM began as research into the application of process improvement and maturity model approaches to security management.

- Literary review and affinity analysis of over 800 standard practices security, BC/DR, and IT ops communities
- Examination of body of knowledge of high-maturity organizations
- Codification of model using trusted CMMI architecture and concepts
- Benchmarking and piloting in the banking/finance community, defense contractors, and US government federal civilian agencies
## CERT-RMM timeline

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004</td>
<td>Began collaboration with FSTC</td>
</tr>
<tr>
<td>2007</td>
<td>CERT Resiliency Engineering Framework v0.95 released</td>
</tr>
<tr>
<td>2008</td>
<td>CERT Resiliency Engineering Framework v0.95 benchmarking effort commenced</td>
</tr>
<tr>
<td>2009</td>
<td>Intro to CERT Resiliency Engineering Framework course piloted</td>
</tr>
<tr>
<td>2010</td>
<td>CERT Resilience Management Model v0.95 released</td>
</tr>
<tr>
<td></td>
<td>CERT Resilience Management Model v1.0 released</td>
</tr>
<tr>
<td></td>
<td>CERT -RMM v1.0 Addison-Wesley book released</td>
</tr>
</tbody>
</table>
Why CERT-RMM?

The rationale for the model
**Imperatives for building CERT-RMM**

- Increasingly complex operational environments where traditional approaches are failing
- Siloed nature of operational risk activities; a lack of convergence
- Lack of common language or taxonomy
- Overreliance on technical approaches
- Lack of means to measure managerial competency
- **Inability to confidently predict outcomes, behaviors, and performance under times of stress**
Organizational challenges

Cope with operational risk and minimize impact

Move all operational risk management activities in the same direction

Optimize cost/effectiveness

Meet mission **no-matter-what**

**How do you measure performance before you’re stressed or fail??**
CERT-RMM Building Blocks

Foundational concepts of the model
Resilience: The physical property of a material when it can return to its original shape or position after deformation that does not exceed its elastic limit [wordnet.princeton.edu]

Operational resilience: The emergent property of an organization exhibited when it continues to carry out its mission after disruption that does not push it beyond its operational limit [CERT-RMM]
Operational resilience & operational risk

Security and business continuity are not end-states; they are continuous processes

Effective operational risk management requires harmonization: convergence of these activities working toward the same goals

Operational resilience emerges from effective operational risk management

- Actions of people
- Systems & technology failures
- Failed internal processes
- External events
Layers of resilience activities

Resilience planning, program execution, and coordination across organizational units

Operational Resilience Management System

Security and Control Activities
- Developing and implementing security architectures, managing security operations

IT Operations Activities
- Developing, implementing, and managing processes to deliver IT services and manage IT infrastructures

Continuity and Recovery Activities
- Developing and executing continuity plans, recovery plans, and restoration plans

Tactical execution of resilience activities
CERT-RMM principle of convergence

Operational resilience is directly affected by convergence

Organizational mission is directly affected by operational resilience
CERT-RMM foundational elements

**Services**
The limited number of activities that the organization carries out in performance of a duty or to produce a product

**Business Processes**
The detailed activities that the organization (and its suppliers) perform to ensure that services meet their mission

**Assets**
Something of value to the organization required by business processes and services to meet their missions
Services in CERT-RMM

The organizing concept in CERT-RMM is a service.

The resilience of high-value services in the organization ensures the resilience of the organization’s mission.

**Service resilience** is a factor of asset resilience—if an asset is disrupted or fails, the service may suffer.

Service resilience is the object of CERT-RMM processes.
Assets

Something of value to the organization

“Charged into production” of business processes and services

Four types of assets are the focus of operational resilience management as defined in CERT-RMM.

- people
- information
- technology
- facilities
Assets charged into production

Asset value relates to the importance of the asset in meeting the business process and service mission.
Operational resilience starts at the asset level

To ensure operational resilience at the service level, related assets must be

- Protected from threats and risks that could disable them
- Made sustainable under adverse conditions

The optimal “mix” of these strategies depends on the value of the asset and the cost of deploying and maintaining the strategy.
Organizational context for resilience activities
CERT-RMM Architecture

*Foundational structures on which the model is built*
CERT-RMM in the life-cycle

Operational resilience management focuses on the deploy, operate, and decommission phases, but reaches back to development phase of lifecycle to ensure consideration of security and continuity issues prior to placing assets in production.
For comparison: CERT-RMM & CMMI

Plan  Operate  Decommission
Design  Develop  Deploy
Acquire  

CERT-RMM

CMMI-DEV
CMMI-ACQ
CMMI-SVC

DEVELOPMENT  OPERATION
CERT-RMM architectural elements

CERT-RMM uses proven architectural elements of CMMI and applies them in an operational context.

- 26 **process areas**
- Arranged in a **continuous representation**
- Goals, practices, sub-practices, and work products that **specifically** define each process area
- Goals, practices, and sub-practices that **generically** define increasing levels of capability
- Implementation and adoption examples
- An **appraisal methodology** to determine capability levels
## CERT-RMM at a glance

### Engineering
<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADM</td>
<td>Asset Definition and Management</td>
</tr>
<tr>
<td>CTRL</td>
<td>Controls Management</td>
</tr>
<tr>
<td>RRD</td>
<td>Resilience Requirements Development</td>
</tr>
<tr>
<td>RRM</td>
<td>Resilience Requirements Management</td>
</tr>
<tr>
<td>RTSE</td>
<td>Resilient Technical Solution Engineering</td>
</tr>
<tr>
<td>SC</td>
<td>Service Continuity</td>
</tr>
</tbody>
</table>

### Enterprise Management
<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMM</td>
<td>Communications</td>
</tr>
<tr>
<td>COMP</td>
<td>Compliance</td>
</tr>
<tr>
<td>EF</td>
<td>Enterprise Focus</td>
</tr>
<tr>
<td>FRM</td>
<td>Financial Resource Management</td>
</tr>
<tr>
<td>HRM</td>
<td>Human Resource Management</td>
</tr>
<tr>
<td>OTA</td>
<td>Organizational Training &amp; Awareness</td>
</tr>
<tr>
<td>RISK</td>
<td>Risk Management</td>
</tr>
</tbody>
</table>

### Operations Management
<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AM</td>
<td>Access Management</td>
</tr>
<tr>
<td>EC</td>
<td>Environmental Control</td>
</tr>
<tr>
<td>EXD</td>
<td>External Dependencies</td>
</tr>
<tr>
<td>ID</td>
<td>Identity Management</td>
</tr>
<tr>
<td>IMC</td>
<td>Incident Management &amp; Control</td>
</tr>
<tr>
<td>KIM</td>
<td>Knowledge &amp; Information Management</td>
</tr>
<tr>
<td>PM</td>
<td>People Management</td>
</tr>
<tr>
<td>TM</td>
<td>Technology Management</td>
</tr>
<tr>
<td>VAR</td>
<td>Vulnerability Analysis &amp; Resolution</td>
</tr>
</tbody>
</table>

### Process Management
<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MA</td>
<td>Measurement and Analysis</td>
</tr>
<tr>
<td>MON</td>
<td>Monitoring</td>
</tr>
<tr>
<td>OPD</td>
<td>Organizational Process Definition</td>
</tr>
<tr>
<td>OPF</td>
<td>Organizational Process Focus</td>
</tr>
</tbody>
</table>

| 26 Process Areas in 4 categories |
Enterprise management

Seven process areas that support the resilience management process

Governance, Risk, & Compliance

Supporting Resilience
Six process areas for establishing resilience for organizational assets, business processes, and services
Operations management

Nine process areas for managing the operational aspects of resilience

Asset Resilience Management

- EC
- KIM
- PM
- TM

Threat, Incident, & Access Management

- AM
- ID
- IMC
- VAR

Supplier Management

- EXD
Process management process areas

Four process areas for defining, planning, deploying, implementing, monitoring, controlling, appraising, measuring, and improving operational resilience management processes

Data Collection & Logging

Process Management
CERT-RMM process area structure

- Focused Activity
- Required
  - What to do to achieve the capability
- Expected
  - How to accomplish the goal
- Informative

Process Area

<table>
<thead>
<tr>
<th>Specific Goals</th>
<th>Generic Goals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specific Practices</td>
<td>Generic Practices</td>
</tr>
</tbody>
</table>

Sub-practices

Maturity Elements

- Purpose Statement
- Introductory Notes
- Related PAs
From "model how" to "tactical how"

Moving from "what" to "how"

The "what"

Process Area

Specific Goals

Specific Practices

Sub-practices

Codes of Practice:
- BS25999-1:2006
- CMMI v1.2
- CMMI for Services
- CobiT 4.1
- COSO ERM
- DRII GAP
- FFIEC Handbooks (Security, BCP)
- ISO 20000-1:2005(E)
- ISO 20000-2:2005(E)
- ISO 24762:2008(E)
- ISO 27001:2005
- NFPA 1600 (2007)
- PCI DSS v1.1
- Val-IT
The Capability Dimension of CERT-RMM

Measuring process institutionalization to determine capability under stress
The promise of process institutionalization

The “capability” dimension of CERT-RMM sets it apart from other models in the operational resilience space

“Capability” determines the degree to which

• A process has been ingrained in the way that work is defined, executed, and managed
• There is commitment and consistency to performing the process

Measuring capability helps you determine the degree to which you are able to control the output of the process—in this case, the degree to which you can predict how well you’ll perform under times of stress
Higher degrees of process institutionalization should translate to more stable processes that

- produce consistent results over time
- are retained during times of stress
Value of knowing your “capability” level

The degree of process institutionalization can help to answer several important questions in managing operational resilience:

- How well are we performing today?
- Can we repeat our successes?
- Do we consistently produce expected results?
- Can we adapt seamlessly to changing risk environments?
- Are our processes stable enough to depend on them under times of stress?
- Can we predict how we will perform under times of stress?

You need to know not only that you’re doing the right things but that you are doing them in a sustainable way.
Process institutionalization in CERT-RMM

Capability levels are used in CERT-RMM to represent process institutionalization.

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

Processes are acculturated, defined, measured, and governed.

Practices are performed.

Practices are incomplete.
Level 0 - Incomplete

Indicates that one or more of the specific goals of the process area is not being achieved

Represents an incomplete process, therefore cannot be institutionalized
Level 1 - Performed

- **Level 3**
  - Defined

- **Level 2**
  - Managed

- **Level 1**
  - Performed

- **Level 0**
  - Incomplete

Represents a **performed** process

Satisfies the specific goals of the process area

Supports and enables the work needed to produce the expected process work products

Provides improvement, but can be lost over time without institutionalization

**Improvements can only be maintained and sustained by moving to higher capability levels (i.e., levels 2 and beyond).**
Level 2 - Managed

Represents a performed process that has the basic infrastructure in place to support the process.

The process is:

- Governed
- Planned and executed in accordance with policy
- Employs skilled people who have adequate resources
- Involves relevant stakeholders
- Is monitored, controlled, and reviewed
- Is evaluated for adherence to its process description

Process discipline ensures that existing practices are retained during times of stress.
Level 3 - Defined

Represents a managed process that is tailored from the organization’s set of standard processes

Contributes work products, measures, and other process improvement information to the organizational process assets

Scope difference from level 2—provides consistency of process assets across organizational units

More rigorous description of processes

**Process management is proactive, not reactive**

Highly important in RMM—because of the “enterprise” and convergence orientation
Capability levels are cumulative

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

Achieving Level 3 means achieving (and sustaining) Level 1 (specific goals) plus Level 2 and Level 3 generic goals, and so on...
## Example: Asset Definition & Management

<table>
<thead>
<tr>
<th>Specific Goals</th>
<th>Specific Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADM:SG1 Establish Organizational Assets</td>
<td>ADM:SG1.SP1 Inventory Assets</td>
</tr>
<tr>
<td></td>
<td>ADM:SG1.SP2 Establish a Common Understanding</td>
</tr>
<tr>
<td></td>
<td>ADM:SG1.SP3 Establish Ownership and Custodianship</td>
</tr>
<tr>
<td>ADM:SG2 Establish Relationship Between Assets and Services</td>
<td>ADM:SG2.SP1 Associate Assets with Services</td>
</tr>
<tr>
<td></td>
<td>ADM:SG2.SP2 Analyze Asset-Service Dependencies</td>
</tr>
<tr>
<td>ADM:SG3 Manage Assets</td>
<td>ADM:SG3.SP1 Identify Change Criteria</td>
</tr>
<tr>
<td></td>
<td>ADM:SG3.SP2 Maintain Changes to Assets and Inventory</td>
</tr>
</tbody>
</table>
## Institutionalizing Asset Definition & Management

<table>
<thead>
<tr>
<th>Specific Goals</th>
<th>Specific Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADM:SG1 Establish Organizational Assets</td>
<td>ADM:SG1.SP1 Inventory Assets</td>
</tr>
<tr>
<td></td>
<td>ADM:SG1.SP2 Establish a Common Understanding</td>
</tr>
<tr>
<td></td>
<td>ADM:SG1.SP3 Establish Ownership and Custodianship</td>
</tr>
<tr>
<td>ADM:SG2 Establish Relationship Between Assets and Services</td>
<td>ADM:SG2.SP1 Associate Assets with Services</td>
</tr>
<tr>
<td></td>
<td>ADM:SG2.SP2 Analyze Asset-Service Dependencies</td>
</tr>
<tr>
<td>ADM:SG3 Manage Assets</td>
<td>ADM:SG3.SP1 Identify Change Criteria</td>
</tr>
<tr>
<td></td>
<td>ADM:SG3.SP2 Maintain Changes to Assets and Inventory</td>
</tr>
</tbody>
</table>

A **managed** process is:

- Governed
- Executed according to policy
- Employs skilled people
- Involves relevant stakeholders
- Monitored, controlled, and reviewed
- Evaluated for adherence to the organization’s process description
- Regularly reviewed with senior management
To institutionalize the performance of the “Inventory Assets” practice, you must commit to and perform these supporting practices:

<table>
<thead>
<tr>
<th>Institutionalizing Factor</th>
<th>Institutionalizing Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governed</td>
<td>There is a policy requiring periodic asset inventory activities; the activity has oversight and corrective actions are taken when necessary</td>
</tr>
<tr>
<td>Employs skilled people</td>
<td>Staff involved in the practice have the appropriate skill levels and training</td>
</tr>
<tr>
<td>Involves stakeholders</td>
<td>Asset owners and custodians are involved; all involved in protecting and sustaining the asset are involved</td>
</tr>
<tr>
<td>Monitored and controlled</td>
<td>The process is measured to determine effectiveness. Examples: % of assets inventoried; # of changes to inventory in a given period</td>
</tr>
<tr>
<td>Evaluate adherence</td>
<td>The process as performed is verified to be aligned with the process definition</td>
</tr>
<tr>
<td>Review with senior management</td>
<td>Keep management informed on the results of the process and identify and resolve issues</td>
</tr>
</tbody>
</table>
Determining Capability using CERT-RMM

Determining an organization’s capability for managing operational resilience
CERT-RMM capability appraisals

An appraisal is used to evaluate (or diagnose) the organization using CERT-RMM as the basis.

The SCAMPI℠ appraisal method from SEI forms the foundation of the CERT-RMM Capability Appraisal Method (RMM CAM)

There are three classes of CERT-RMM appraisals:

- **CAM Class A**: Most rigorous
- **CAM Class B**: Performed by Team
- **CAM Class C**: Most flexible
- **Official rating**
- **Unofficial Results**

One appraiser
CERT-RMM capability survey

A self-directed assessment instrument that provides a quick organizational “health check”

Low investment, but potentially high impact

Can be used to catalyze a more formal process improvement effort

Currently in development; to be released by year-end 2010

Not considered to be one of the “class” appraisals and not based on the SCAMPI method
Value of a CERT-RMM appraisal

Process improvement model can allow for third-party appraisals

Creation of a set of professionals skilled in rating process performance

Elimination of subjectivity in rating process performance and institutionalization

Ability to provide statistics on organization and industry capability levels
Appraisal scope

The depth of the CERT-RMM appraisal can vary depending on the organization’s objectives. (i.e., It can simply help the organization to determine where it is or it can lead to a formal capability level rating.)

Can include one process area or a group of process areas

- Can be broad:
  - One process area over many operational units
- Or deep:
  - Many process areas in one operational unit
Appraisal scope

Appraisal Scope = Organizational Unit + Model Scope

Key CMMI differences:
- No “project” in CERT-RMM
- Instantiations will vary at the practice level

Key CMMI difference:
- Fine-grained CERT-RMM scoping options

May be a subset of improvement scope
Appraisal scope: capability profile

Capability Profile

ADM
Asset Definition & Mgmt

COMP
Compliance

IMC
Incident Mgmt & Control

KIM
Knowledge & Info Mgmt

TM
Technology Mgmt

0 1 2 3

target

target

target

target
Appraisal results may indicate gaps.

Gaps should be analyzed and prioritized prior to implementing improvements.
CERT-RMM Credentialing
Certifying CERT-RMM professionals
CERT-RMM professional roles

CERT-RMM Appraiser

CERT-RMM Navigator
CERT-RMM Coach
CERT-RMM Appraisal Team Member

These roles are under development—priority will be based on demand
CERT-RMM Appraiser

SEI-Certified CERT-RMM Appraisers can lead all classes (A, B, and C) of appraisals including the Capability Survey.

The CERT-RMM Appraiser is responsible to plan and manage the performance of the entire appraisal effort, delegate appraisal tasks to team members, and ensure adherence to CAM appraisal requirements.

CERT-RMM Appraisers are sponsored by SEI Partners who are licensed to perform activities on behalf of the SEI.
CERT-RMM Coach

Employees or consultants who are assigned to apply, analyze, champion, manage, contribute, or support CERT-RMM based improvement efforts, appraisal teams, and/or organizational initiatives

Provide a workforce element that will promote a smooth adoption of CERT-RMM concepts to create a sustainable improvement effort

Can deliver CERT-RMM class B or C appraisals and the Capability Survey
CERT-RMM Navigator

Provide guidance and management of organizations who are applying the CERT-RMM Capability Survey

Coordinator between the organization and the SEI on completion of the Survey and reporting results from the SEI to the organization

Can only deliver the CERT-RMM Capability Survey; no Class appraisals
# CERT-RMM credentialing summary

<table>
<thead>
<tr>
<th>Role</th>
<th>Authorizations</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>CERT-RMM Appraiser</td>
<td>--Class A, B, and C</td>
<td>Reserved for existing CMMI Lead Appraisers only at this time;</td>
</tr>
<tr>
<td></td>
<td>--Capability Survey</td>
<td>--Intro to CERT-RMM course</td>
</tr>
<tr>
<td></td>
<td></td>
<td>--CERT-RMM CAM BootCamp</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2011 Program in development for “new” appraisers</td>
</tr>
<tr>
<td>CERT-RMM Coach</td>
<td>--Class B and C</td>
<td>--Intro to CERT-RMM course</td>
</tr>
<tr>
<td></td>
<td>--Capability Survey</td>
<td>--CERT-RMM Coach Training</td>
</tr>
<tr>
<td>CERT-RMM Navigator</td>
<td>--Capability Survey</td>
<td>--Intro to CERT-RMM course</td>
</tr>
<tr>
<td></td>
<td></td>
<td>--CERT-RMM Navigator Training</td>
</tr>
<tr>
<td>CERT-RMM Appraisal Team</td>
<td>Performs as member of</td>
<td>--Intro to CERT-RMM course</td>
</tr>
<tr>
<td>Member</td>
<td>appraisal team</td>
<td>--CERT-RMM Appraisal Team Training</td>
</tr>
</tbody>
</table>
CERT-RMM and PS-Prep

Comparing and contrasting CERT-RMM in the context of FEMA’s PS-Prep program
What is PS-Prep?

FEMA’s Voluntary Private Sector Preparedness Accreditation and Certification Program

Mandated by Title IX of the 9/11 Commission Act of 2007

Participation is completely voluntary

DHS approved three standards in June 2010:

- National Fire Protection Association 1600
- British Standard 25999 – Business Continuity Management

ANSI-ASQ National Accreditation Board will oversee the certification process
“Prepared” vs. “Capable”

**PS-Prep**: promote private sector preparedness “including disaster management, emergency management, and business continuity programs.”

**CERT-RMM**: promote private sector capability—preparedness is a function of:

- Protection strategies (preventative)
- Sustainability strategies (responsive)
- Process institutionalization or “maturity” to determine the degree to which these strategies will “stick” when the organization is stressed

**Prepared**: can you respond?

**Capable**: can you control your destiny by heading off problems and responding when stressed?
## CERT-RMM vs. ASIS standard -2

A preliminary comparison:

<table>
<thead>
<tr>
<th>Area of Comparison</th>
<th>CERT-RMM</th>
<th>ASIS SPC.1-2009</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scope</strong></td>
<td>Security, continuity, IT operations; takes management system view but also addresses key operational activities such as vulnerability management, access management, and identity management; also addresses resilience in the development and acquisition phases</td>
<td>Focuses on the organizational resilience management system and key management processes</td>
</tr>
<tr>
<td><strong>Process approach</strong></td>
<td>Uses CMMI’s process structure; uses “process” as the dimension for measurement of capability; processes are arranged into process areas to allow for scalable and agile adoption</td>
<td>Defines process approach broadly in terms of a “plan-do-check-act model”</td>
</tr>
<tr>
<td><strong>Maturity considerations</strong></td>
<td>Uses proven CMMI capability dimension for maturity expression; some process areas express maturity dimensions as well</td>
<td>Includes “maturity” elements, but does not appear to have a maturity representation analogous to CMMI or CERT-RMM</td>
</tr>
<tr>
<td><strong>Appraisal</strong></td>
<td>Appraisal against the model uses proven SCAMPI method for CMMI; significant installed base of qualified and experienced appraisers; official “capability level”</td>
<td>Includes an assessment process specific to determining compliance with the standards; no maturity rating</td>
</tr>
</tbody>
</table>
CERT-RMM scorecard

Advantages:

- **One model** with significant coverage of standards
- Ability to **incorporate any useful standard/practice**
- Capability dimension provides
  - proven **maturity path**
  - ability to determine degree to which practices are retained under stress
- Focuses on **process improvement** not just certification; has a built-in path to improvement
- Allows for **process-based metrics and measurement**

Advantages:

- Creates **internal process improvement experts** to sustain competency
- Appraisal and certification model established and proven; **issued ratings “sanctioned” by the SEI/CERT**

Disadvantage:

- Limited coverage of emergency/crisis management (for now)
CERT-RMM Product Suite

Model artifacts available to begin an adoption process
## CERT-RMM product suite

<table>
<thead>
<tr>
<th>Product</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>CERT-RMM Model</td>
<td>Version 1.0 released; Technical Report released; individual process areas released @ <a href="http://www.cert.org/resilience">www.cert.org/resilience</a></td>
</tr>
<tr>
<td>CERT-RMM Capability Appraisal Methodology</td>
<td>Version 1.0 to be released in method description document, August 2010</td>
</tr>
<tr>
<td>CERT-RMM Crosswalk</td>
<td>Version 0.95 published; Version 1.0 (expanded) to be published late Summer</td>
</tr>
<tr>
<td>Introductory courses</td>
<td>Introduction to CERT-RMM (4 days; offered 4 times/year in Pittsburgh and DC) Executive workshops and tutorials available on demand</td>
</tr>
<tr>
<td>Advanced courses</td>
<td>CERT-RMM Intermediate Course (in development for 2011)</td>
</tr>
<tr>
<td></td>
<td>CERT-RMM CAM BootCamp (pilot scheduled for November 2010)</td>
</tr>
<tr>
<td></td>
<td>CERT-RMM Role training (Coach, Navigator)</td>
</tr>
<tr>
<td></td>
<td>CERT-RMM instructor training</td>
</tr>
</tbody>
</table>
CERT-RMM book publication

Scheduled for publication in November 2010 by Addison-Wesley

Includes full model (v1.0) plus adoption guidance and perspectives of real-world use of the model
Resilience measurement & analysis

Area of research growing out of CERT-RMM development

Focuses on the development of adequate measures to determine transformation of operational resilience management system

Focuses on performance measurement—how well are we doing?

Includes both qualitative and quantitative measurements

Measurement users group (RMM MUG) forming—Fall 2010 opportunity to join a measurement cohort and share
Questions?
CERT-RMM contacts

Rich Caralli
RMM Architect and Lead Developer
rcaralli@cert.org

David White
RMM Transition Lead & Developer
dwhite@cert.org

Lisa Young
RMM Appraisal Lead & Developer
lry@cert.org

Julia Allen
RMM Developer/Measurement Team Lead
jha@sei.cmu.edu

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

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

SEI Customer Relations
customer-relations@sei.cmu.edu
412-268-5800
NO WARRANTY

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE 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.

Use of any trademarks in this presentation is not intended in any way to infringe on the rights of the trademark holder.

This Presentation 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.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.
Want a Closer Connection to the SEI?

Become an SEI Member!

www.sei.cmu.edu/membership
CERT's Podcast Series: Security for Business Leaders

www.cert.org/podcast/
For more than 20 years, the SEI has been at the forefront of software engineering.

By becoming an SEI Partner, you join forces with a software engineering pioneer and an institute whose credibility provides a solid foundation during uncertain economic times.

SEI Partner Network

www.sei.cmu.edu/partners
Do you have the knowledge you need?

SEI Training

www.sei.cmu.edu/training