Using CERT-RMM in a Software and System Assurance Context

Julia Allen
SEPG NA 2011
24 March 2011
Agenda

What is the CERT Resilience Management Model (CERT-RMM)?

Model Building Blocks

CERT-RMM for Assurance
What is CERT-RMM?

The CERT® Resilience Management Model is a maturity model for managing and improving operational resilience.

- Process improvement for operational resilience
- Converges key operational risk management activities: security, BC/DR, and IT operations
- Operations phase focus
- CMMI architecture
- Continuous representation
- 26 process areas
- Defines maturity through capability levels
CERT-RMM Building Blocks

Foundational concepts of the model
Operational resilience

**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:** An *emergent* property
Operational resilience and operational risk

Operational resilience emerges from effective operational risk management

Operational risk categories:

- Actions of people
- Systems and technology failures
- Failed internal processes
- External events
CERT-RMM foundational elements
Services in CERT-RMM

The resilience of high-value services ensures the resilience of the 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

CERT-RMM focuses on four types:

- People
- Information
- Technology
- Facilities
Assets supporting the mission
Operational resilience starts at the asset level

Protect assets from threats

Make them sustainable under adverse conditions

Optimal mix depends on the value of the asset and the cost of deploying and maintaining the strategy
Organizational context for resilience activities
CERT-RMM for Assurance

Focusing CERT-RMM on early life-cycle activities for building resilience in
CERT-RMM focus in the life cycle

Assets in Production
For comparison: CERT-RMM and CMMI

- Plan
- Develop
- Acquire
- Design
- Deploy
- Operate
- Retire

CERT-RMM

CMMI-DEV

CMMI-ACQ

CMMI-SVC

DEVELOPMENT

OPERATION
RTSE – Resilient Technical Solution Engineering

Ensure that software and systems are developed to satisfy their resilience requirements
## RTSE specific goals

<table>
<thead>
<tr>
<th>Goal</th>
<th>Goal Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTSE:SG1</td>
<td>Establish guidelines for resilient technical solution development</td>
</tr>
<tr>
<td>RTSE:SG2</td>
<td>Develop resilient technical solution development plans</td>
</tr>
<tr>
<td>RTSE:SG3</td>
<td>Execute the plan</td>
</tr>
</tbody>
</table>
RTSE: Building in versus bolting on

Requires organizational intervention

Extends resilience requirements to assets that are to be developed

Creates requirements for quality attributes

Attempts to reduce the level of operational risk

Extends across the life cycle
RTSE: Design and test for resilience

- Perform resilience controls during planning and all life cycle phases
- Specify and maintain resilience requirements
- Design resilience-specific architectures
- Adopt secure coding practices
- Minimize weaknesses and vulnerabilities (defects)
- Design test criteria to attest to asset resilience
- Test for resilience during assembly and integration
- Design and exercise service continuity plans during the development process
RTSE influences

**BSIMM2**
bsimm.com

Open Web Applications Security Project (OWASP)
**Software Assurance Maturity Model**
www.owasp.org

**Microsoft Security Development Life Cycle**
www.microsoft.com/security/sdl/

**DHS Process Reference Model for Assurance Mapping to CMMI-DEV V1.2**
https://buildsecurityin.us-cert.gov/swa/procrsrc.html
CERT-RMM for software assurance
## CERT-RMM assurance view

<table>
<thead>
<tr>
<th>Engineering</th>
<th>Operations Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADM</td>
<td>AM</td>
</tr>
<tr>
<td>CTRL</td>
<td>EC</td>
</tr>
<tr>
<td>RRD</td>
<td>EXD</td>
</tr>
<tr>
<td>RRM</td>
<td>ID</td>
</tr>
<tr>
<td>RTSE</td>
<td>IMC</td>
</tr>
<tr>
<td>SC</td>
<td>KIM</td>
</tr>
<tr>
<td></td>
<td>PM</td>
</tr>
<tr>
<td></td>
<td>TM</td>
</tr>
<tr>
<td></td>
<td>VAR</td>
</tr>
<tr>
<td>Enterprise Management</td>
<td>Process Management</td>
</tr>
<tr>
<td>COMM</td>
<td>MA</td>
</tr>
<tr>
<td>COMP</td>
<td>MON</td>
</tr>
<tr>
<td>EF</td>
<td>OPD</td>
</tr>
<tr>
<td>FRM</td>
<td>OPF</td>
</tr>
<tr>
<td>HRM</td>
<td></td>
</tr>
<tr>
<td>OTA</td>
<td></td>
</tr>
<tr>
<td>RISK</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Framing process to practice

Moving from “what” to “how”
Example – Training and Awareness

Goal: Establish and maintain the strategic assurance training needs of the organization.

Process areas: OTA, RTSE, HRM

CERT-RMM Subpractices

- BSIMM2
- OpenSAMM
- Microsoft SDL

Training related practices for creating the software security satellite, role-based training on demand . . .

Practices for technical security awareness training. . .

Training guidelines on basic concepts, common baseline, training topics. . .
CERT-RMM links to codes of practice

Process Area

The “what”

Specific Goals

Moving from “what” to “how”

Specific Practices

From “model how” to “tactical how”

Codes of Practice:
- BS25999-1: 2011
- CMMI v1.2
- CMMI for Services
- CobiT 4.1
- COSO ERM
- DRII GAP
- FFIEC BCP Handbook
- ISO 20000-2:2005
- ISO 24762:2008
- ISO 27002:2005
- NFPA 1600 (2007)
## Resources

### Training

*Introduction to the CERT Resilience Management Model (3-day course)*
- Public courses (Pittsburgh and DC)
- Private onsite courses

Appraiser and instructor training in development

**CERT-RMM User Group Annual Series**
- Quarterly 2-day workshops
- Focus on CERT-RMM implementation
- CERT-RMM Coach Certification option

### Book

Includes full model (v1.1) plus adoption guidance and perspectives of real-world use of the model


### Website

[www.cert.org/resilience](http://www.cert.org/resilience)

### Support

Engage CERT-RMM team to lead appraisals, provide implementation coaching, pilot CERT-RMM Compass, or deliver custom training

© 2011 Carnegie Mellon University
CERT-RMM contacts

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

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

Lisa Young  
RMM Appraisal Lead and 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

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

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

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

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.

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