CERT-RMM and SSE CMM

Table of Contents

CERT ® Resilience Management Model (CERT ® - RMM)................................................................. 2
CERT-RMM ...................................................................................................................................... 3
Operational Lifecycle Context......................................................................................................... 6
CERT-RMM Organizational Context -1............................................................................................ 8
CERT-RMM Organizational Context -2............................................................................................ 9
CERT-RMM at a glance.................................................................................................................. 10
SSE Capability Maturity Model ..................................................................................................... 11
Notices .......................................................................................................................................... 13
Another option that you can use is the Resilience Management Model, also done here at SEI.
CERT-RMM

A capability model for managing and improving operational resilience

• Guides implementation and management of operational resilience activities
• Converges security, BC/DR, and IT operations activities
• Defines maturity through capability levels (like CMMI)
• Improves confidence in how an organization manages and responds to operational stress
• Reaches back to inform security and continuity as development requirements

“…an extensive super-set of the things an organization could do to be more resilient.”
- CERT®-RMM adopter

**043 The RMM really gives you a--it's a capability model for managing and improving operational resilience. What did we say operational resilience is? Remember the spring, right? As you stretch a spring and let go out of it, it'll snap back to where it was before. If you stretch a spring too far, you hear that thunk, and now you've broken your spring. Same thing with your business, right? As you're going down the road and bouncing down the Yellow Brick Road here, operational resilience gives you the ability to react to various events, until you hit something that exceeds your limit, and then you break.
But RMM gives you kind of an implementation guide, a way of doing resilience activities within your organization. Remember, operational resilience isn't something that you do in and of itself; it's something that comes out of all of the things that you do-- all of the things you do holistically within your organization. So you do risk management, you do business continuity, you do continuous monitoring. All those sorts of things give you operational resilience.

Remember the diagram where we had security, IT operations and business continuity? Where all those three things converge, that's resilience, and that's what this is trying to get you to do, is all three of those.

So it also defines maturity levels, kind of like the capability maturity model. It will say, "You are doing not so good," "Managed," "You're doing great," "You have best-in-class processes because you're able to continuously improve them." So this gives you a way to not only do resilience or achieve operational resilience, but it'll tell you how far along you are in that process. It'll give you a scoring guide, if you will, through the maturity model.

It should give you confidence in the fact that your organization is able to weather bumps in the road or operational stress, I think is the term that's used in here. So if you're able to respond to that operational stress,
you should have confidence in the fact that you can actually do that, that you can actually survive it.

And hopefully what you get out of the resiliency process here will help you improve your risk management process, your continuity processes, and your own security processes, because those become-- what you learn from the resiliency process here can become requirements to your security process, or your security infrastructure, your lifecycle.
**044 If you look at kind of where this fits within a lifecycle model-- at the top of this chart there’s a typical lifecycle, where if you start over here on the left you've got planning. Start with the requirement, right? Now I’m planning. How do I-- or, "What do I do about this requirement? Do I design something? Do I develop something? Do I acquire something, go out and buy it?" Then you move into deploying. Then you operate it for a while. And eventually you get to the point where you unplug it from the wall and you toss it in the dumpster. You retire it.
So, some of the capability maturity models that are out there only focus on development, which is from the middle of the slide over to the left, or they focus on operation. I think one of the benefits of RMM is that it focuses across the-- it focuses on both the development aspects of it and the operational aspects of it.

Why is this important? We did talk about the fact that when is it a good time to integrate security into a process or a product-- is it before you buy it, after you've bought it, or after you've implemented it?

Student: Before you buy it.

Chris Evans: Before you buy it.
Right. Where does everybody do it? After they've implemented it. "Oh yeah, we forgot security. We got to put that in here." But RMM basically says that: Bake security in from the beginning and follow it all the way through to the point that you toss it in the trash. You'll end up with a much more resilient organization if you do that.
Four asset types:

- People – the human capital of the organization
- Information – data, records, knowledge in physical or digital form
- Technology – software, systems, hardware, network
- Facilities – offices, data centers, labs – the physical places

So again, RMM focuses on development capabilities. So, assets in production and actually assets that have been deployed or in operation, so in production. RMM is going to focus on these four things here. We’re talking about people, information, technology, and facilities. So those are the general categories of critical assets that you could have in your organization. And so RMM is going to focus on those four areas.
And it's going to say that for each of those areas, look at how to protect that particular asset, and also how to sustain it. So, what's the difference between protecting and sustaining? What's this kind of line down the center between protection and sustaining?

Student: Would that be protect before something happens, and then sustain after something happens?

Chris Evans: Yep. So the big bang happens right here in between these two areas. So, protection measures are things that you do before that operational stress occurs. So, how
do you reduce your risk, how do you reduce the impact of it to these particular areas-- that's, how do you protect these particular assets? Sustainment is, "Okay, something happened to my facility. How do I continue? How do I carry on my business? How do I sustain that asset if I can? Or how do I sustain my business practices based on something bad happening to one of these particular assets?"

**CERT-RMM at a glance**

<table>
<thead>
<tr>
<th>Engineering</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADM  Asset Definition and Management</td>
<td>AM  Access Management</td>
</tr>
<tr>
<td>CTRL  Controls Management</td>
<td>EC  Environmental Control</td>
</tr>
<tr>
<td>RRD  Resilience Requirements Development</td>
<td>EXD  External Dependencies Management</td>
</tr>
<tr>
<td>RRM  Resilience Requirements Management</td>
<td>ID  Identity Management</td>
</tr>
<tr>
<td>RTSE  Resilient Technical Solution Engineering</td>
<td>IMC  Incident Management and Control</td>
</tr>
<tr>
<td>SC  Service Continuity</td>
<td>KIM  Knowledge and Information Management</td>
</tr>
<tr>
<td></td>
<td>PM  People Management</td>
</tr>
<tr>
<td></td>
<td>TM  Technology Management</td>
</tr>
<tr>
<td></td>
<td>VAR  Vulnerability Analysis and Resolution</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Enterprise Management</th>
<th>Process Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMM  Communications</td>
<td>MA  Measurement and Analysis</td>
</tr>
<tr>
<td>COMP  Compliance</td>
<td>MON  Monitoring</td>
</tr>
<tr>
<td>EF  Enterprise Focus</td>
<td>OPD  Organizational Process Definition</td>
</tr>
<tr>
<td>FRM  Financial Resource Management</td>
<td>OPF  Organizational Process Focus</td>
</tr>
<tr>
<td>HRM  Human Resource Management</td>
<td></td>
</tr>
<tr>
<td>OTA  Organizational Training and Awareness</td>
<td></td>
</tr>
<tr>
<td>RISK  Risk Management</td>
<td></td>
</tr>
</tbody>
</table>

**047 RMM has a very large practice area, so it defines 26 processes within four different categories, and it will give you**
strategies and ideas for looking at
technology management with relation
to those four asset categories that
we talked about in the previous
section.

SSE Capability Maturity Model

SSE Capability Maturity Model

Systems Security Engineering Capability Maturity Model

- Employment of existing processes (e.g., CMMI, CERT-RMM)
- Addresses security engineering activities
- Owners are
  - Developers
  - Integrators
  - System users
  - Organizations
- Applies to all security engineering related activities

“It is a model that should not be practiced in a vacuum.”

- Everyone must participate or its not effective

**048 And the last one here that
we’ll talk about-- the System Security
Engineering Capability Model. This is
like a maturity model, but for systems
security. And the essential parts of
this are you have to involve different
folks. You have to involve developers;
you have to involve integrators; you have
to involve people who use this system;
and actually, you have to involve the
organization as a whole.
What is this trying to do? It's trying to say that security engineering should be involved-- sorry-- each of these people, or groups of people, should be involved in security engineering. Who are the developers? They're the people who create this monstrosity. Right? Well, if they're not thinking about security, what do you end up with? You end up with a product that you've now bought that security hasn't been baked into it. If the integrators, the people who are deploying this system into a workplace or something like that, aren't thinking about security, what do you have? You've got a system, you've got that Polycom device that gets dropped on a desk and, "Okay, here you go." "Oh, wait, we ought to tell the security guys about it."

So the point behind the security engineering process is that it's a model that should not be practiced in a vacuum, and it takes everyone in that list-- developers, integrators, users, management within the organization-- to support this process. Otherwise it's just not effective, and you end up with implementations that are not secure.
Notices

© 2014 Carnegie Mellon University

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

This material 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 U.S. government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. government purposes, the SEI recommends attendance to ensure proper understanding.

THE MATERIAL IS PROVIDED ON AN "AS IS" BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

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