

CERT Resilience Management Model Overview

Table of Contents

CERT-RMM	2
Operational Lifecycle Context	4
CERT-RMM Organizational Context -1	5
CERT-RMM Organizational Context -2	6
CERT-RMM at a glance	7
Notices	8

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



**046 Instructor: So, this is a capability model that helps you maintain resilience in your enterprise. Recall, when we talked about the idea of knowing your uncertainties-- and this is a chicken and egg principle. If I understand risk, I can make myself have a more resilient enterprise. That is, when that cold dark day comes, I can recover and keep my operation going so that way the organization isn't brought to its knees, and hopefully it can withstand any given incident.

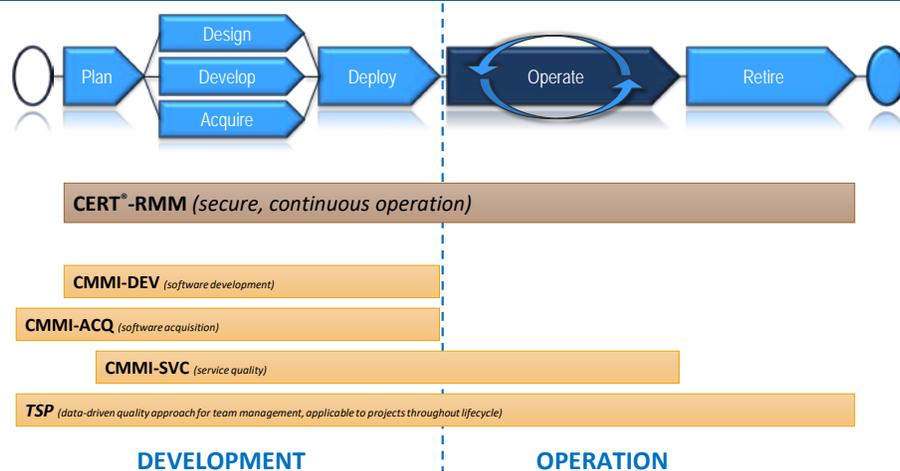
RMM helps you do that. It helps guide you through how you would manage these activities related to planning for resilience, how you're going to actually implement it. And following even incidents, there some business continuity disaster recovery elements to it. And it all circles

around an IT operations context. It also helps you measure the maturity that you may have within that process. You can also understand how confident you would be at meeting any given stress that is provided to the enterprise, and it helps you reach back and keep the organization more informed about what you're doing about continuity in the enterprise.

Now, RMM is big. There's a lot to it. So, I'd like to pause here to note that you shouldn't feel compelled to ingest all of the Resilience Management Model, all of RMM, and feel like you have to do it all at once. As a matter of fact, we're going to talk a little bit about this here in the future, but what I would like to know is if you were to go and Google RMM and find it at the SEI website, you can download the textbook. And it is massive.

Operational Lifecycle Context

Operational Lifecycle Context



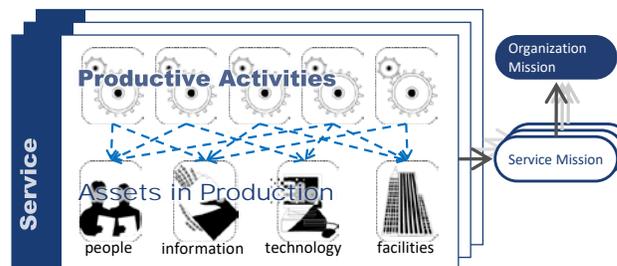
47

**047 That said, I don't want you to be overwhelmed. Rather, what I want you to do is understand the basis of where it came from and the elements that might help you best. This slide kind of helps you with that idea. It looks at the idea of the existing assets that the SEI has published in the past, especially around the capability and maturity models, and it will actually help you understand, too, that RMM rests upon the principles and ideas that came out of all those great products with the goal of having a more secure enterprise that can maintain operations despite that darkest day taking place. And you're going to go through this process again and again. With any given asset that you have, you're going to plan to have it. You're going to design, develop it. You're going to actually bring it in the

enterprise and ingest it and start using it. You're going to deploy it in the enterprise. And then your longest phase right there may be to operate it. And then eventually you're going to retire it. And you're going to have to understand how you're going to do all that within the context of having it in terms of if a risk were to come to fruition.

CERT-RMM Organizational Context -1

CERT-RMM Organizational Context -1



■ 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

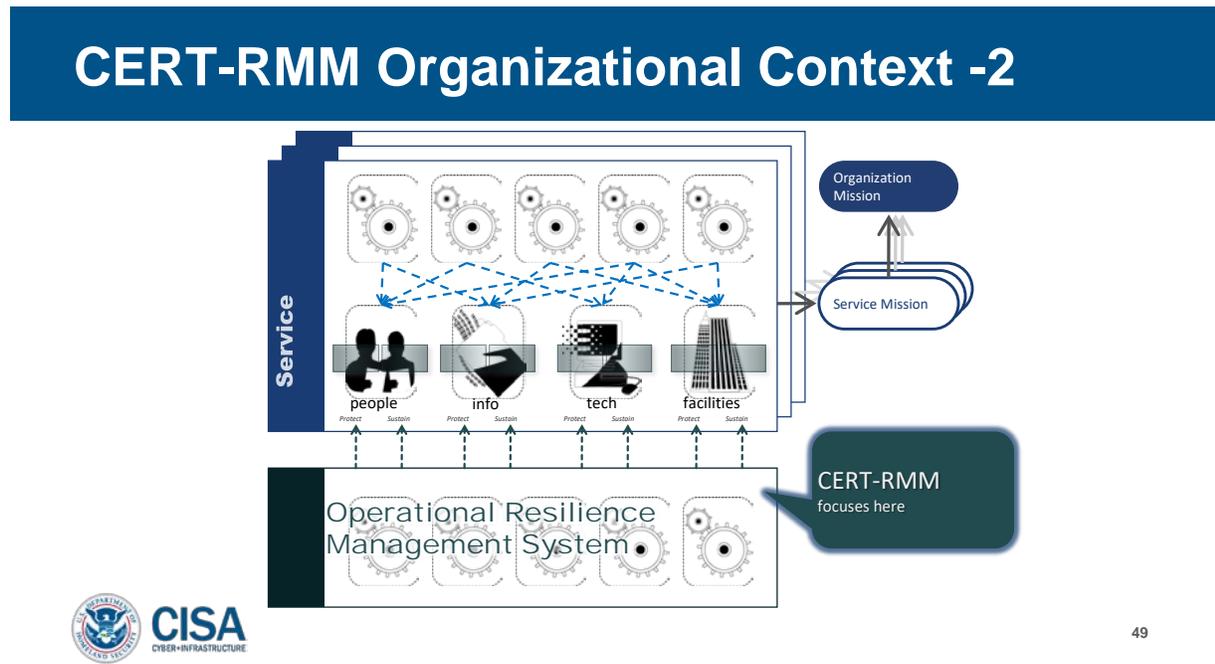


48

**048 RMM does a really good job at categorizing assets in your business. Asset management is key to good risk management. There are four types of assets. There are people, information, technology, and facilities. It's interesting to note here, too, that you could also think about each of those elements in a third-party context. So, don't forget just about the assets that you have in your enterprise. You want to also

think about the service providers that you may have that serve as critical assets to your organization as well.

CERT-RMM Organizational Context -2



**049 Furthermore, what you want to do is focus on each of those asset types, understand how they are critical to the enterprise, what critical services they are delivering, understand the risk related to it and what you are going to specifically do to make sure that those assets are protected. So, that way, when that risk comes to light, you could still be resilient and keep your organization operating.

CERT-RMM at a glance

CERT-RMM at a glance

26 Process Areas in 4 categories

Engineering	
ADM	Asset Definition and Management
CTRL	Controls Management
RRD	Resilience Requirements Development
RRM	Resilience Requirements Management
RTSE	Resilient Technical Solution Engineering
SC	Service Continuity

Enterprise Management	
COMM	Communications
COMP	Compliance
EF	Enterprise Focus
FRM	Financial Resource Management
HRM	Human Resource Management
OTA	Organizational Training and Awareness
RISK	Risk Management

Operations	
AM	Access Management
EC	Environmental Control
EXD	External Dependencies Management
ID	Identity Management
IMC	Incident Management and Control
KIM	Knowledge and Information Management
PM	People Management
TM	Technology Management
VAR	Vulnerability Analysis and Resolution

Process Management	
MA	Measurement and Analysis
MON	Monitoring
OPD	Organizational Process Definition
OPF	Organizational Process Focus



50

**050 RMM does this in a very interesting way. It breaks down into 26 process areas under four different categories. Now, here's where you can get slightly overwhelmed. Each of these process areas within the textbook, or within the training, however you ingest RMM, you're going to find out that there's a lot to each given step. You're going to have to actually sit down and reflect upon what your enterprise needs most first. Maybe you need to characterize what your operations are first because that's what you're doing to actually physically getting the product out the door. So, categorically, you start there. And maybe only pick several process areas.

So, that way, you can make yourself better at maybe identity management or maybe your environmental controls.

Maybe access is an issue for you, maybe how you actually manage your assets or your people. So, you focus there first, and then you would branch out and start thinking about the other process areas within those categories that may need some focus so that way you can make your enterprise, over time, far more resilient.

Notices

Notices

Copyright 2019 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

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.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution. This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study. Except for any U.S. government purposes described herein, 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. 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.

DM18-0098



1