



Capability Maturity Models and Insider Risk Deterrence

Matthew Butkovic

Technical Director-Cyber Risk and Resilience

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Marking

Copyright 2024 Carnegie Mellon University.

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 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.

CERT® and Carnegie Mellon® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM24-1647

Presenter Overview

Matthew Butkovic, CISSP, CISA

- Technical Director-Cyber Risk and Resilience (CERT Division-Software Engineering Institute-CMU-Carnegie Mellon University)
- Adjunct Faculty-Heinz College (Policy and Governance)
- Instructor-Heinz College CISO, CIO, and CRO Executive Education Certificate Program
- Adjunct Faculty- CMU Institute for Strategy and Technology
- Private Industry Prior to CMU (Banking and Manufacturing)



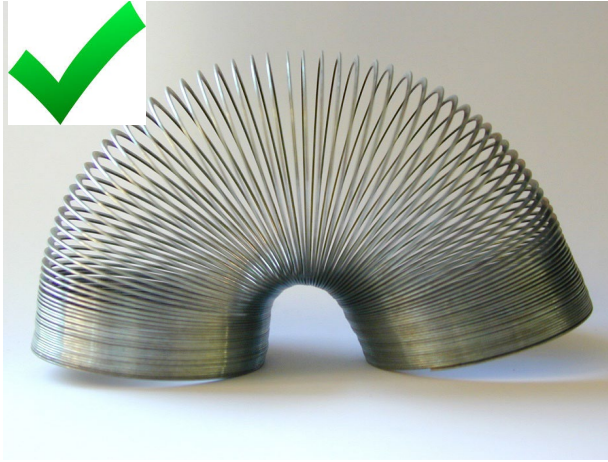
Operational Resilience Defined

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* that can *continue to carry out its mission* after *disruption* that *does not exceed* its *operational* limit[CERT-RMM]



Like a Slinky....



<https://www.youtube.com/watch?v=EZL6RGkPjws>



Operational Resilience Reminder



Verisk's PCS Classifies CrowdStrike Incident as a Cyber Catastrophe

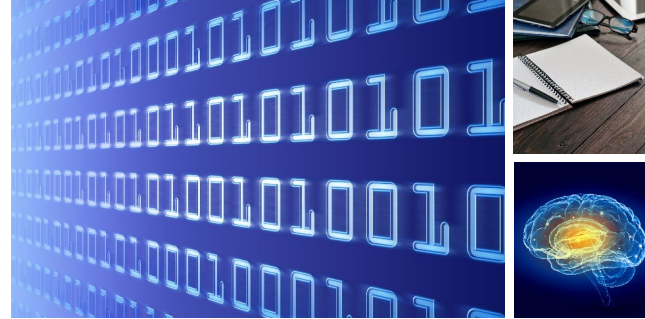
By [Chad Hemenway](#) | July 31, 2024



Asset Types Essential to Operational Resilience



Technology



Information

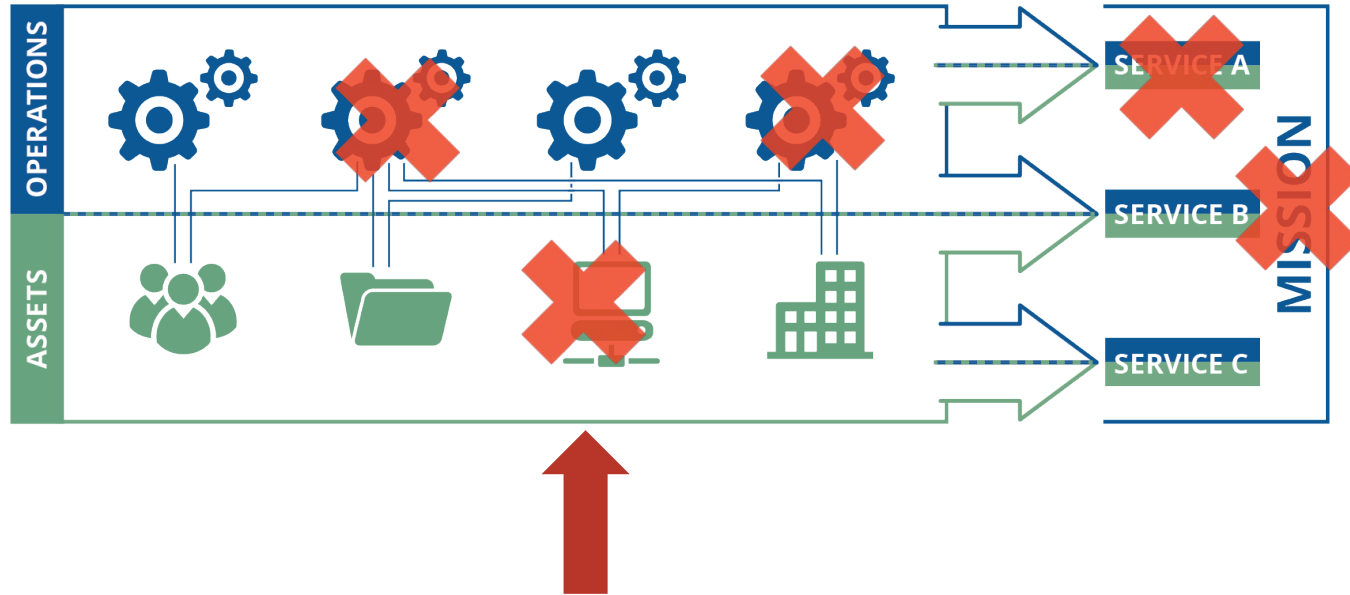


People



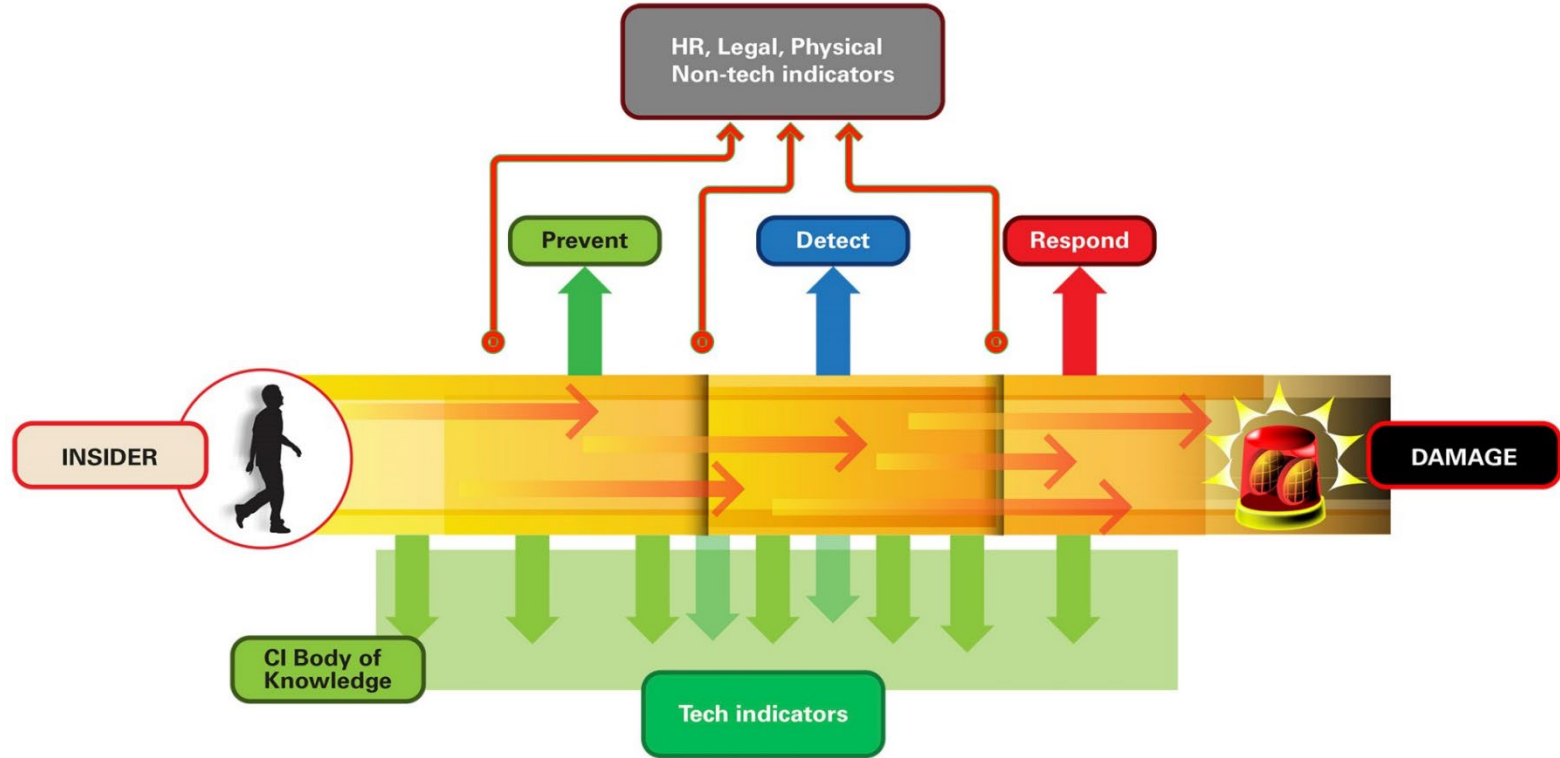
Facilities

Disruption of Assets Can Lead to Mission Failure



**Realized operational risk resulting
in asset disruption**

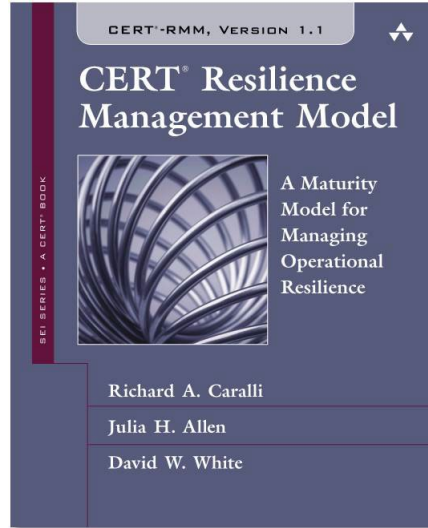
The Goal for an Insider Threat Program...



Is to reduce insider risks to critical assets to acceptable levels

<https://insights.sei.cmu.edu/insider-threat/2020/01/maturing-your-insider-threat-program-into-an-insider-risk-management-program.html>

CERT Resilience Management Model (CERT-RMM)



Framework for managing and improving operational resilience

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

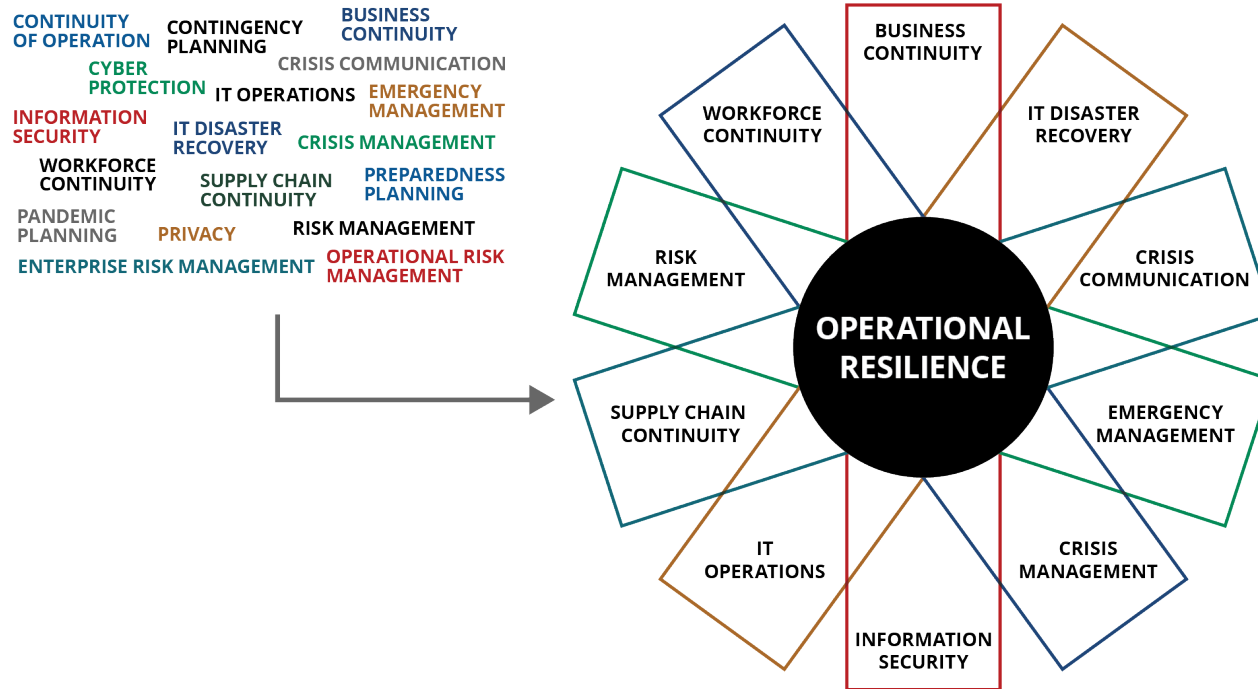
“...an extensive super-set of the things an organization could do to be more resilient.”

- CERT-RMM adopter

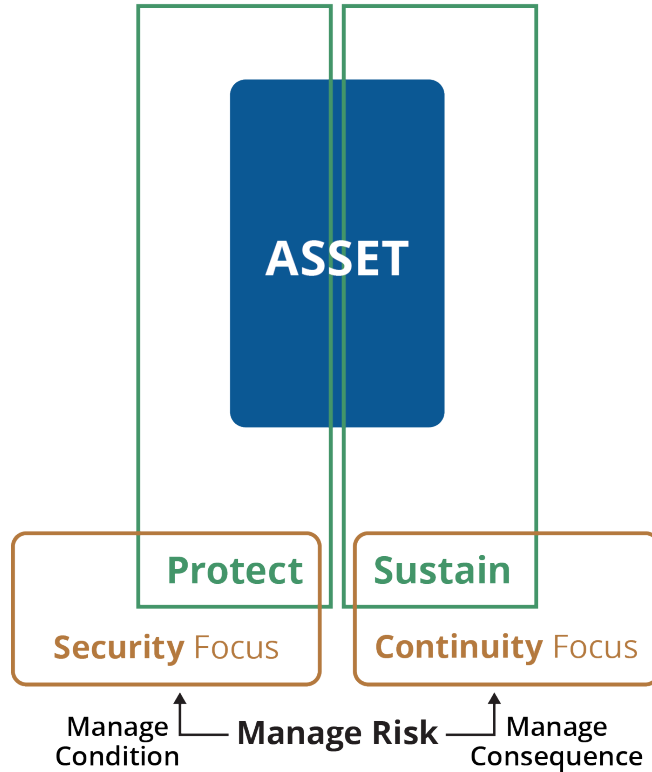
A Sampling of CERT-RMM Applications and Derivatives



Desired Integrated Approach



Efficiency

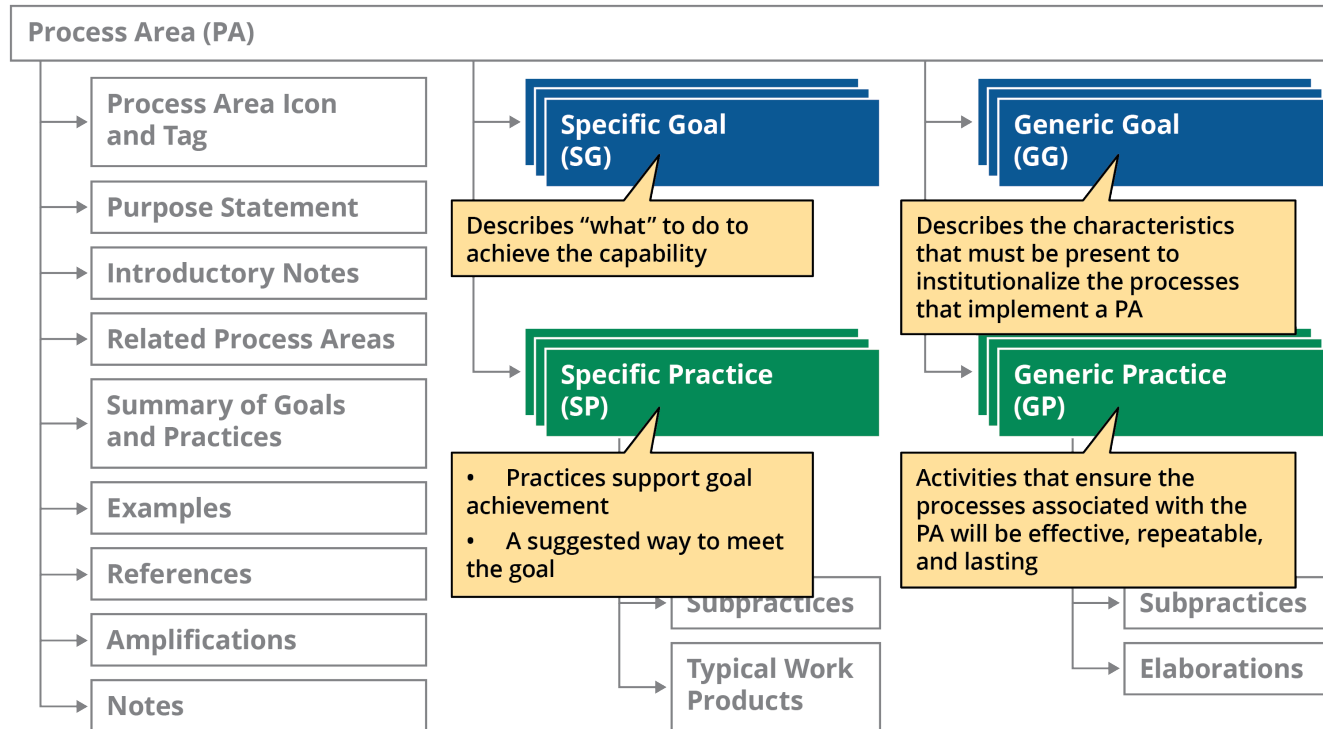


The optimal mix of protection and sustainment strategies

Depends on the **value** of the asset to the service and the **cost** of deploying and maintaining the strategy

The management challenge of operational resilience

RMM Structure & Components



CERT-RMM by the Numbers



RMM Categories and Process Areas

Engineering		Operations	
ADM	Asset Definition and Management	AM	Access Management
CTRL	Controls Management	EC	Environmental Control
RRD	Resilience Requirements Development	EXD	External Dependencies Management
RRM	Resilience Requirements Management	ID	Identity Management
RTSE	Resilient Technical Solution Engineering	IMC	Incident Management and Control
SC	Service Continuity	KIM	Knowledge and Information Management
Enterprise Management		PM	People Management
COMM	Communications	TM	Technology Management
COMP	Compliance	VAR	Vulnerability Analysis and Resolution
EF	Enterprise Focus	Process Management	
FRM	Financial Resource Management	MA	Measurement and Analysis
HRM	Human Resource Management	MON	Monitoring
OTA	Organizational Training and Awareness	OPD	Organizational Process Definition
RISK	Risk Management	OPF	Organizational Process Focus

Where Insider Threat Programs Traditionally Focus

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	

Where Insider Threat Programs Need To Expand

Engineering			Operations		
ADM	Asset Definition and Management	★	AM	Access Management	
CTRL	Controls Management		EC	Environmental Control	★
RRD	Resilience Requirements Development	★	EXD	External Dependencies Management	★
RRM	Resilience Requirements Management	★	ID	Identity Management	
RTSE	Resilient Technical Solution Engineering	★	IMC	Incident Management and Control	
SC	Service Continuity	★	KIM	Knowledge and Information Management	★
Enterprise Management			PM	People Management	★
COMM	Communications		TM	Technology Management	
COMP	Compliance	★	VAR	Vulnerability Analysis and Resolution	
EF	Enterprise Focus		Process Management		
FRM	Financial Resource Management		MA	Measurement and Analysis	
HRM	Human Resource Management		MON	Monitoring	
OTA	Organizational Training and Awareness		OPD	Organizational Process Definition	★
RISK	Risk Management	★	OPF	Organizational Process Focus	★

Questions



Resources and Tools for Operational Resilience Management

- CERT Resilience Management Model
 - <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419>
- RMM Code of Practice Crosswalk
 - <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508084>
- RMM NIST SP 800 Series Crosswalk
 - <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=93044>
- Operationally Critical Threat, Asset, and Vulnerability Evaluation
 - <https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=309051>
- CERT Common Sense Guide to Mitigating Insider Threats
 - <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=540644>