



Applying the CERT[®] Resilience Management Model to the Counter-Insider Threat Mission

Dan Costa

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

Copyright 2020 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense 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.

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.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

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.

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

Operationally Critical Threat Asset and Vulnerability EvaluationSM is a service mark of Carnegie Mellon University.

DM20-0609

Operational Resilience

Operational resilience: The *emergent property* of an organization that can continue to carry out its mission in the presence of operational *stress* and *disruption* that does not exceed its limit.

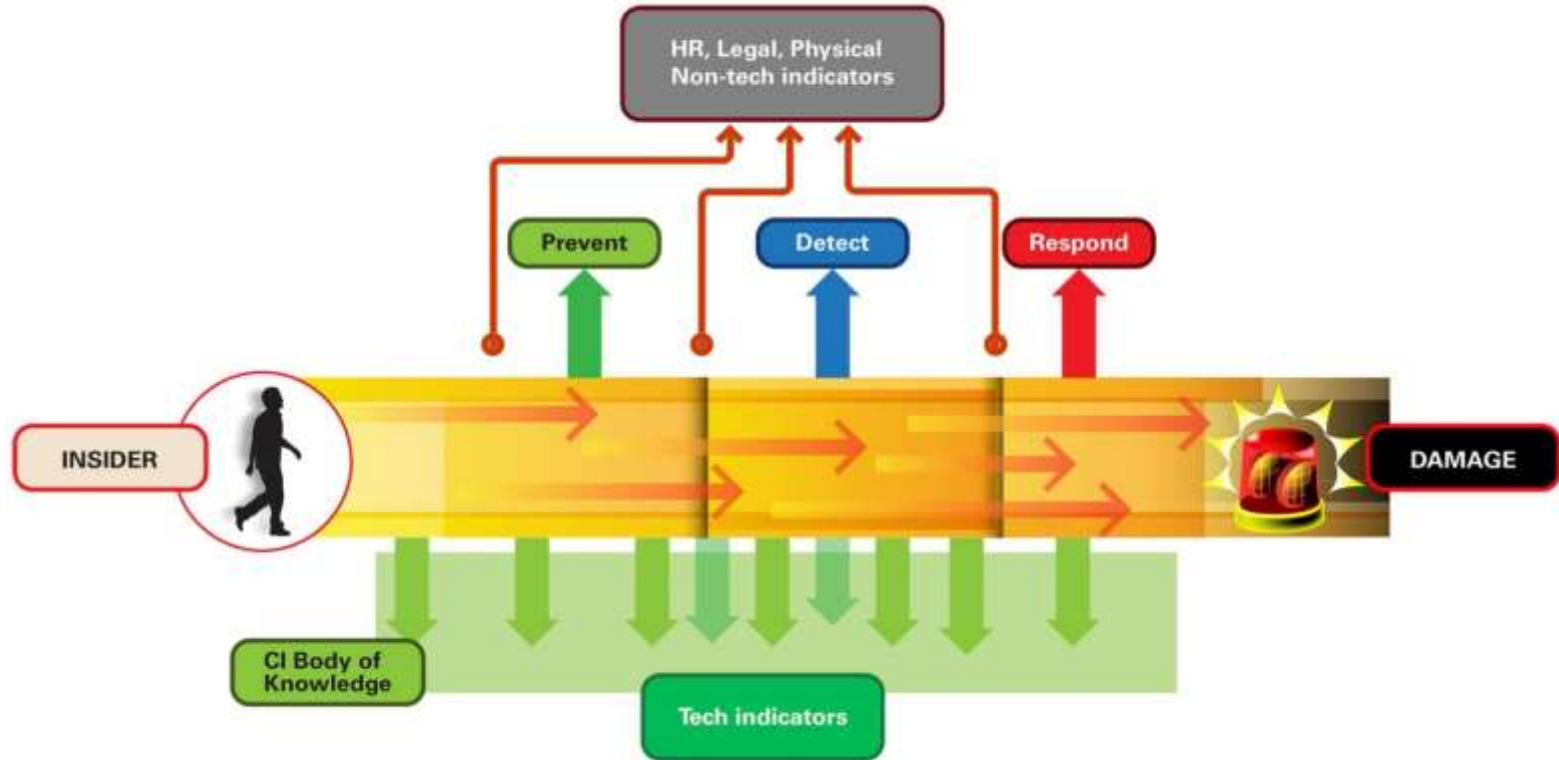
Stress and *disruption* come from **risk**

Risk is the impact and likelihood associated with a threat occurring

Operational resilience emerges from effective **risk management**



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>

“Acceptable Levels”? Quantifiable and Actionable Risk Appetite Statements for Likelihood and Impact

Executive Attention

- Threat is between 75-99% likely to occur within the next year, or has occurred within the industry in the last year

Management Attention

- Threat is between 30-74% likely to occur within the next year, or has occurred within the industry in the last two years

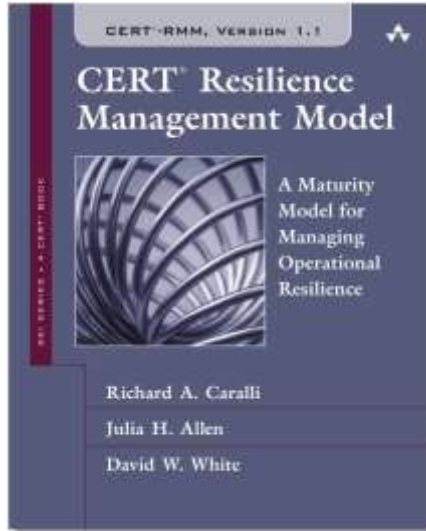
Front Line Attention

- Threat is between 1-29% likely to occur within the next year, or has occurred within the industry in the last 5 years

	Revenue (Operating Profit)	Safety	Operations	Reputation	Compliance	Human Capital	Projects
Escalate to Executive Attention	Any more than a 10% deviation from planned operating profit for a quarter	Loss of life or permanent disability	No more than three days of lost operations	Loss of market segment with multiple customers	Debarment from a particular market segment linked to regulatory violation(s)	Any more than 5% high performer attrition from any business unit in a quarter	Liquidated damages that exceed contract value
Escalate to Management Attention	Any more than a 5% deviation from planned operating profit for a quarter	Time away or other reportable incident	No more than one day of lost operation	Loss of customer	Any fines or other penalties linked to regulatory violation(s)	Any more than 3% high performer attrition from any business unit in a quarter	Liquidated damages that erode the margin as sold
Provide Front Line Attention	Any deviations from planned operating profit for a quarter	Bumps, strains, bruises	No more than one shift of lost operation	Customer complaints or negative social media buzz	Any warnings linked to regulatory violation(s)	Any developing trend in high performer attrition	Minor disputes with limited contractual impact

<https://www.rsaconference.com/industry-topics/presentation/finding-the-right-answersfacilitating-insider-threat-analysis-using-octave>

CERT Resilience Management Model (CERT-RMM)



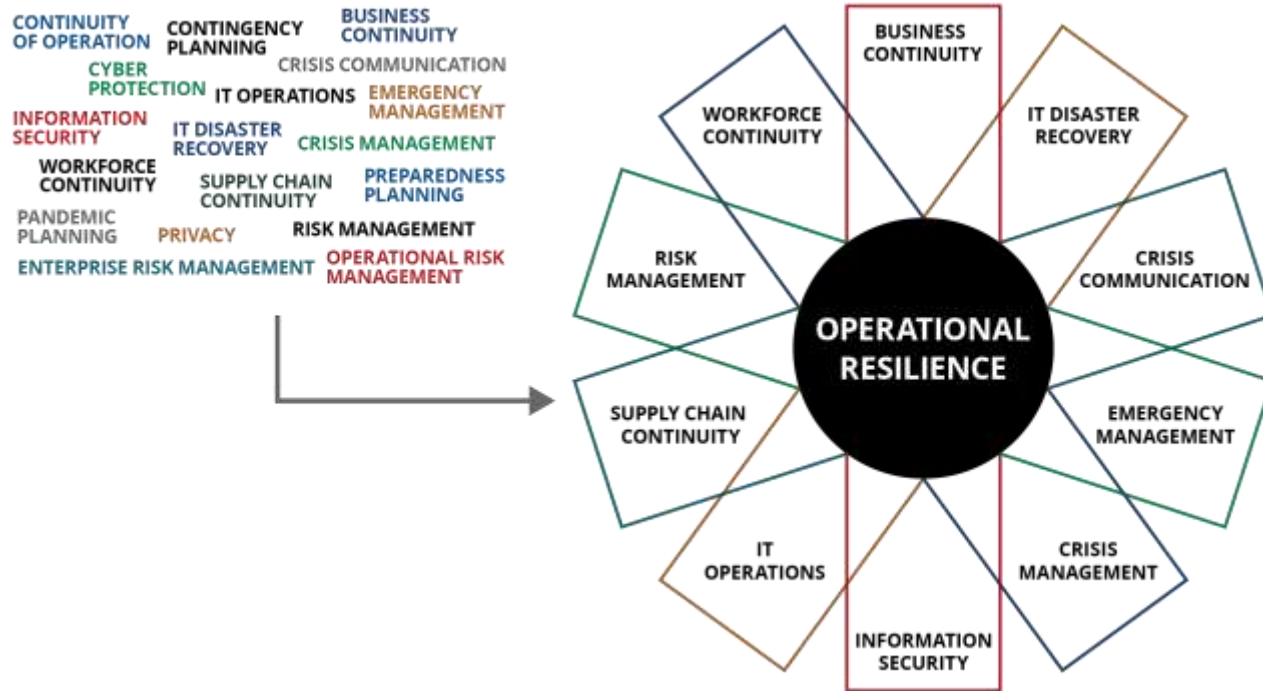
<http://www.cert.org/resilience>

Framework for managing and improving operational resilience

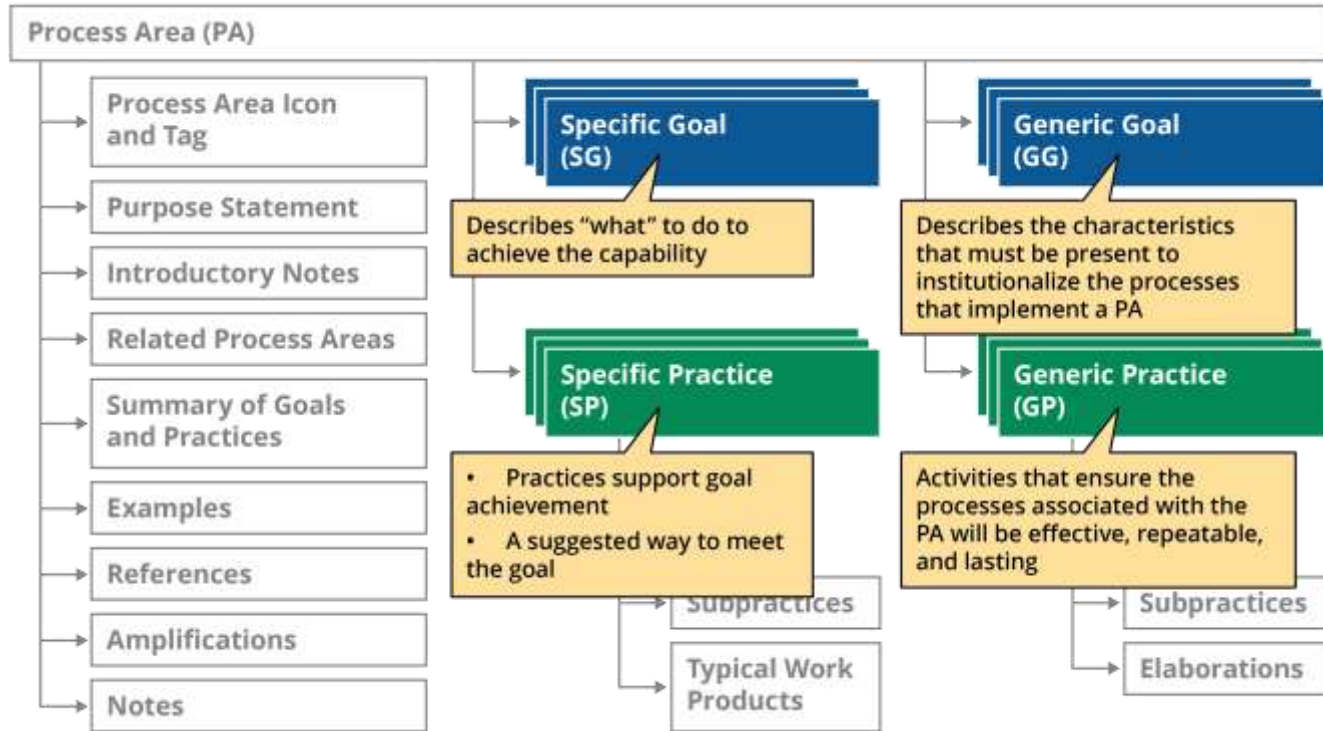
“...an extensive super-set of the things an organization could do to be more resilient.”

- CERT-RMM adopter

Desired Integrated Approach



RMM Structure & Components



CERT-RMM by the Numbers



RMM Categories and Process Areas

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 Traditionally Focus

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 Need To Expand

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 ★

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>

Conclusion

The Counter-Insider Threat Program of the future is an integrated, proactive, risk-based mission enabler that makes its organization operationally resilient against insider threats.



How do we get there?

- By expanding relationships with traditionally under-represented insider threat program stakeholders
- By clearly articulating program goals and risk appetite
- By placing an emphasis on process institutionalization, yielding more stable processes that produce consistent results over time that are retained during times of stress

Presenter Contact Information

Dan Costa, CISSP

Technical Manager, CERT National Insider Threat Center

dlcosta@sei.cmu.edu