



# From Mitigating Insider Threats to Managing Insider Risk

Dan Costa

Sarah Miller

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](mailto:permission@sei.cmu.edu).

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

DM20-0714

# Where InTP's Have Succeeded

- Connecting the dots
- Technical detection of blatant policy violations
- Identifying broken business processes




# Where InTP's Are Struggling




- Measures of Effectiveness / ROI
- Scoping
- Change management
- Proactive responses to the conditions that precede harmful acts






# Where Insider Threat Programs Traditionally Focus

| Engineering |   |
|-------------|---|
| <b>ADM</b>  | Asset Definition and Management   |
| <b>CTRL</b> | Controls Management  |
| <b>RRD</b>  | Resilience Requirements Development   |
| <b>RRM</b>  | Resilience Requirements Management  |
| <b>RTSE</b> | Resilient Technical Solution Engineering  |
| <b>SC</b>   | Service Continuity  |



  

| Enterprise Management |   |
|-----------------------|---|
| <b>COMM</b>           | Communications                         |
| <b>COMP</b>           | Compliance  |
| <b>EF</b>             | Enterprise Focus                       |
| <b>FRM</b>            | Financial Resource Management          |
| <b>HRM</b>            | Human Resource Management              |
| <b>OTA</b>            | Organizational Training and Awareness  |
| <b>RISK</b>           | Risk Management   |

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

| Process Management |  |
|--------------------|--|
| <b>MA</b>          | Measurement and Analysis  |
| <b>MON</b>         | Monitoring                |
| <b>OPD</b>         | Organizational Process Definition  |
| <b>OPF</b>         | Organizational Process Focus   |

# Where Insider Threat Programs Need To Expand

| Engineering |  |
|-------------|--|
| <b>ADM</b>  | Asset Definition and Management ★          |
| <b>CTRL</b> | Controls Management                        |
| <b>RRD</b>  | Resilience Requirements Development ★      |
| <b>RRM</b>  | Resilience Requirements Management ★       |
| <b>RTSE</b> | Resilient Technical Solution Engineering ★ |
| <b>SC</b>   | Service Continuity ★                       |

| Enterprise Management |                                       |
|-----------------------|---------------------------------------|
| <b>COMM</b>           | Communications                        |
| <b>COMP</b>           | Compliance ★                          |
| <b>EF</b>             | Enterprise Focus                      |
| <b>FRM</b>            | Financial Resource Management         |
| <b>HRM</b>            | Human Resource Management             |
| <b>OTA</b>            | Organizational Training and Awareness |
| <b>RISK</b>           | Risk Management ★                     |

| Operations |  |
|------------|--|
| <b>AM</b>  | Access Management                      |
| <b>EC</b>  | Environmental Control ★                |
| <b>EXD</b> | External Dependencies Management ★     |
| <b>ID</b>  | Identity Management                    |
| <b>IMC</b> | Incident Management and Control        |
| <b>KIM</b> | Knowledge and Information Management ★ |
| <b>PM</b>  | People Management ★                    |
| <b>TM</b>  | Technology Management                  |
| <b>VAR</b> | Vulnerability Analysis and Resolution  |

| Process Management |                                     |
|--------------------|-------------------------------------|
| <b>MA</b>          | Measurement and Analysis            |
| <b>MON</b>         | Monitoring                          |
| <b>OPD</b>         | Organizational Process Definition ★ |
| <b>OPF</b>         | Organizational Process Focus ★      |

# 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.

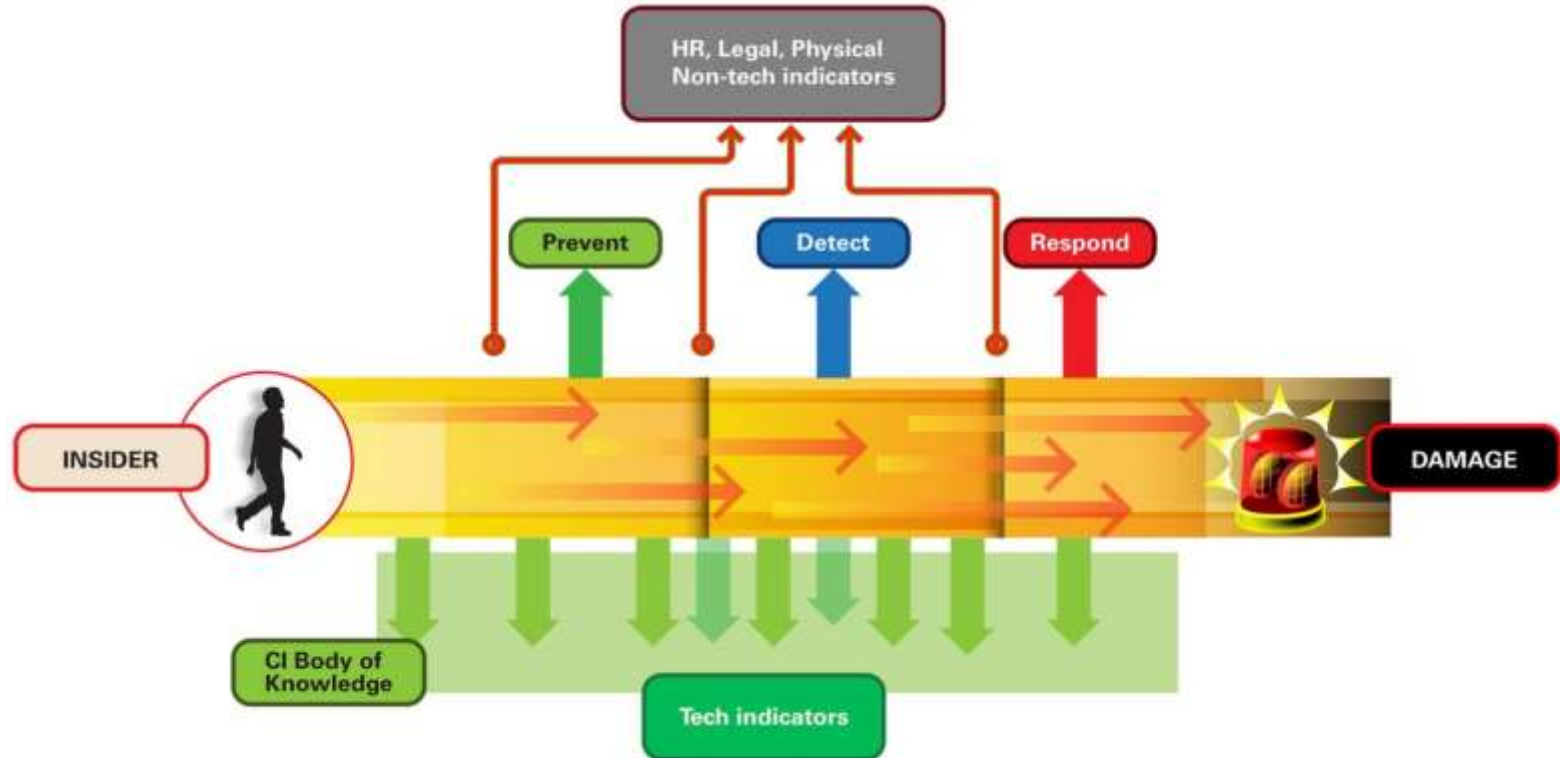
*Stress* and *disruption* come from **risk**

**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>

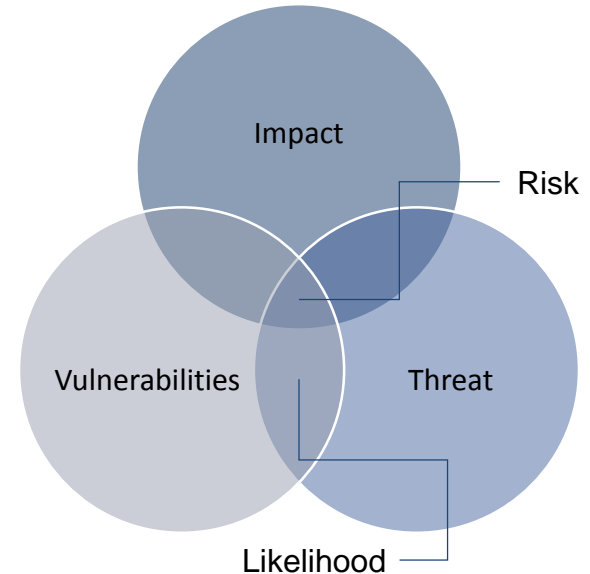
# Acceptable Levels?

Risks can be expressed as a function of **impact** and **likelihood**

Deploying controls doesn't necessarily reduce the likelihood of a threat occurring, especially for insider threats.

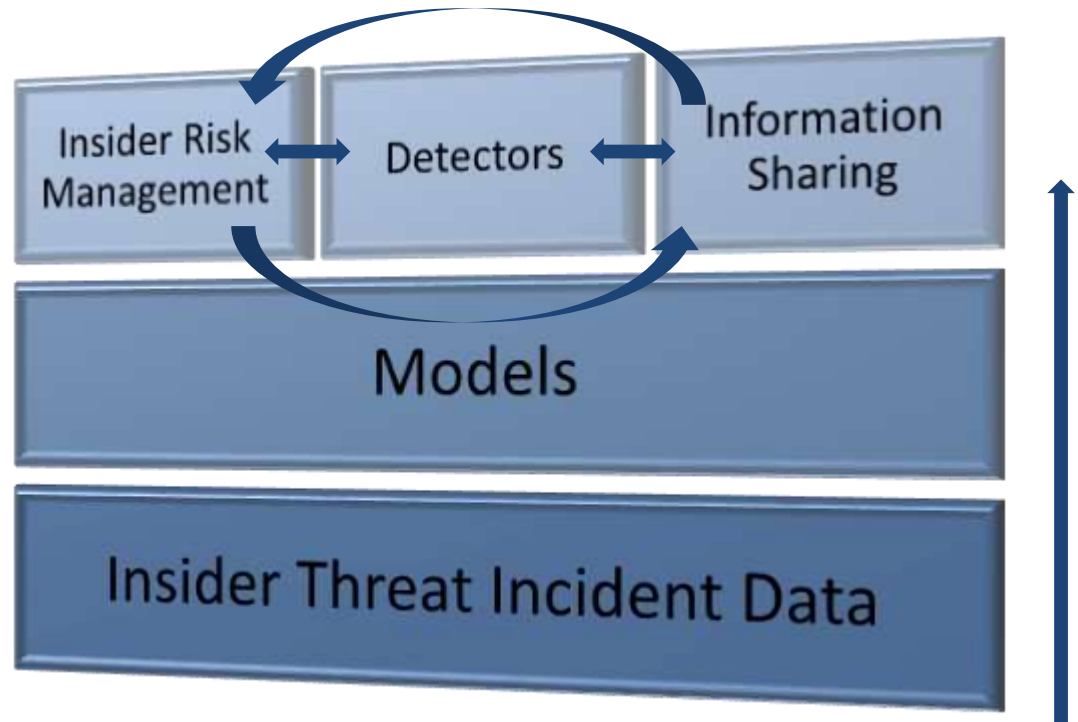
How much insider risk is our organization willing or able to withstand while still carrying out its mission?

- To begin to answer this question, we need quantifiable and actionable **risk appetite statements**
  - To do this, we need reliable, sound methods for measuring the likelihood and impact of insider threats



# How Do We Get There?

- Business impact analysis
- Continuous measurement of current security posture
- Broadening the scope of what's considered a 'security control'
- Using our data
- Information sharing



# Conclusion

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



This future state can be realized by:

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