#RSAC

RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **HUM-M03**

# Stop Chasing Insider Threats, Start Managing Insider Risk

**Randy Trzeciak**

Technical Director, Security Automation
CERT Division, Software Engineering Institute,
Carnegie Mellon University
rft@sei.cmu.edu

# Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

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.

References herein to any specific commercial product, process, or service by trade name, trademark, 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.

DM21-1083

# Presentation Objectives

- Identify the state of insider risk/threat mitigation today
- Identify components of a holistic insider risk management program
- Identify how (and why) to ground the insider threat problem and solutions in the principles of enterprise and cyber risk management

# State of Insider Threat Mitigation

- 59% of organizations prioritize external threats over internal ones
- 59% of incidents in the last 12 months caused by insiders
- 58% do not have a dedicated insider threat team
- 39% of organizations lack the necessary budget; 38% lack internal expertise; 29% don’t see insiders as a “substantial threat”
- *70% of organizations don’t have an insider risk management strategy*

Source: December 2021 Forrester, commissioned by Imperva; Insider Threats Drive Data Protection Improvement, Threat Detection, analytics, And Staffing Lead Investment Priorities; https://www.imperva.com/resources/resource-library/white-papers/forrester-insider-threats-drive-data-protection-improvements-full-report/

# Have These Ever Happened To You?

- Having trouble clearly stating the scope of your organization's insider threat program?
- Struggling with fully capturing the value and effectiveness of your organization's insider threat program?
- Lacking organization-wide consensus regarding your organization's security posture against insider threats?
- Having difficulty providing actionable intelligence to your insider threat program stakeholders?

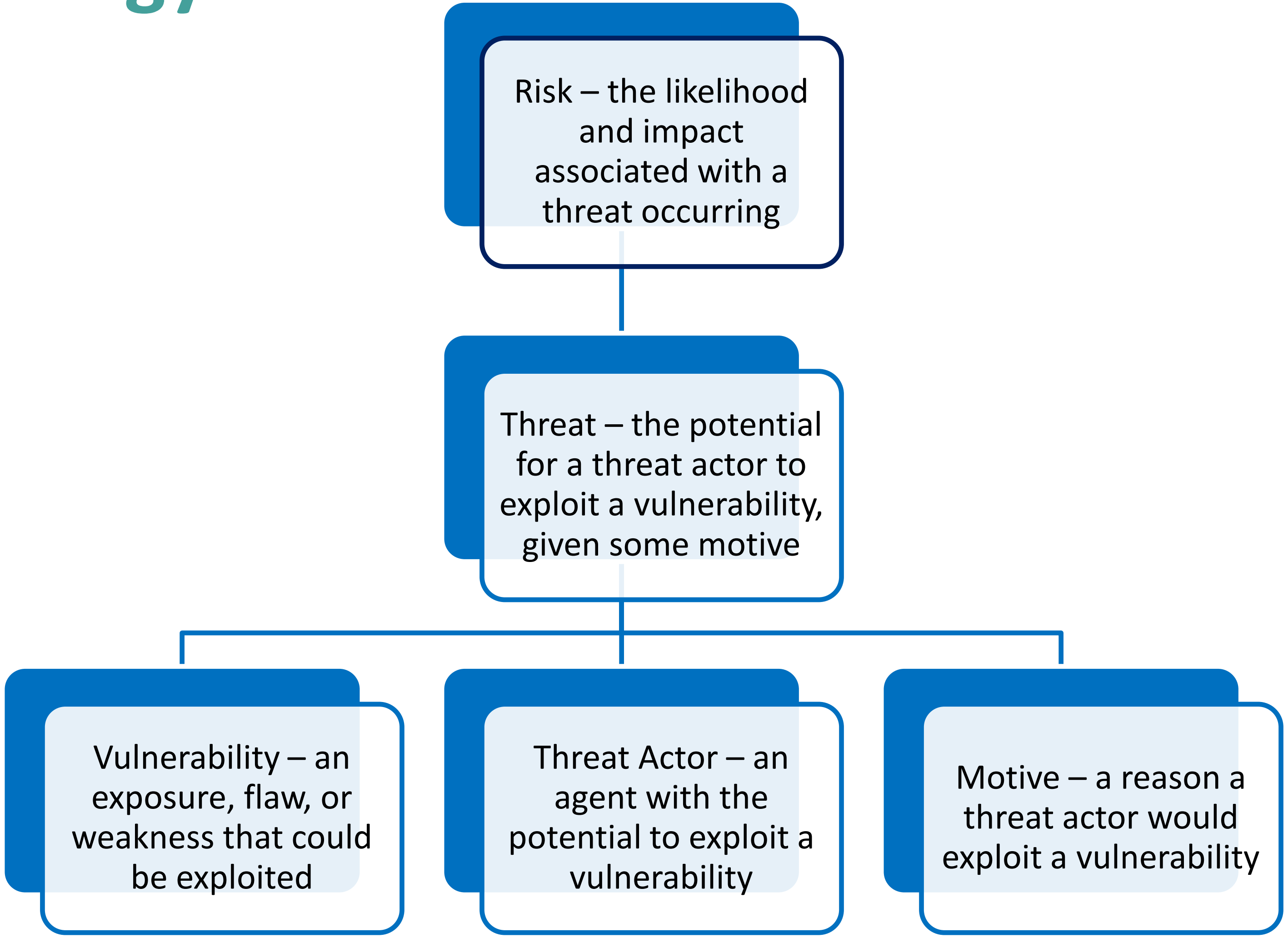
These are all signs that your organization's insider threat program may need a big change.

# Insider Risk Management Principles

# 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. [CERT-RMM]
- *Stress* and *disruption* come from **risk**
- Operational resilience emerges from effective **risk management**

# Risk Terminology



Risk – the likelihood and impact associated with a threat occurring

Threat – the potential for a threat actor to exploit a vulnerability, given some motive

Vulnerability – an exposure, flaw, or weakness that could be exploited

Threat Actor – an agent with the potential to exploit a vulnerability

Motive – a reason a threat actor would exploit a vulnerability

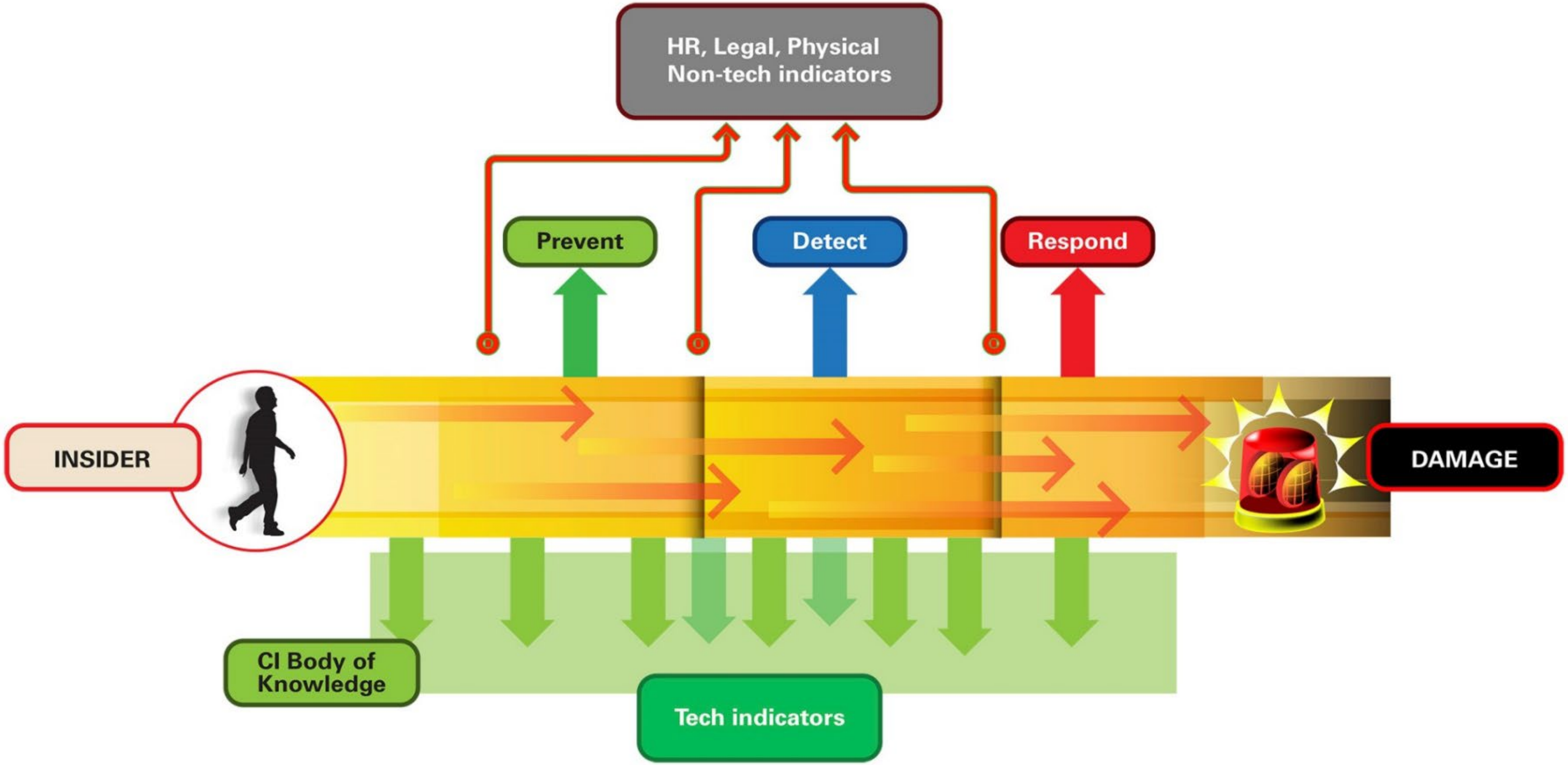
Definitions adapted from the CERT® Resilience Management Model

# Managing Risks

- Risk management – The continuous process of identifying, analyzing, and addressing risks to organizational assets that could adversely affect the operation and delivery of services. [CERT-RMM]

- Risk management is an enterprise-wide activity that involves:
  - Identifying mission-critical assets
  - Identifying threats to assets
  - Assessing impact and likelihood of threats occurring
  - Creating and implementing plans for reducing risks to acceptable levels

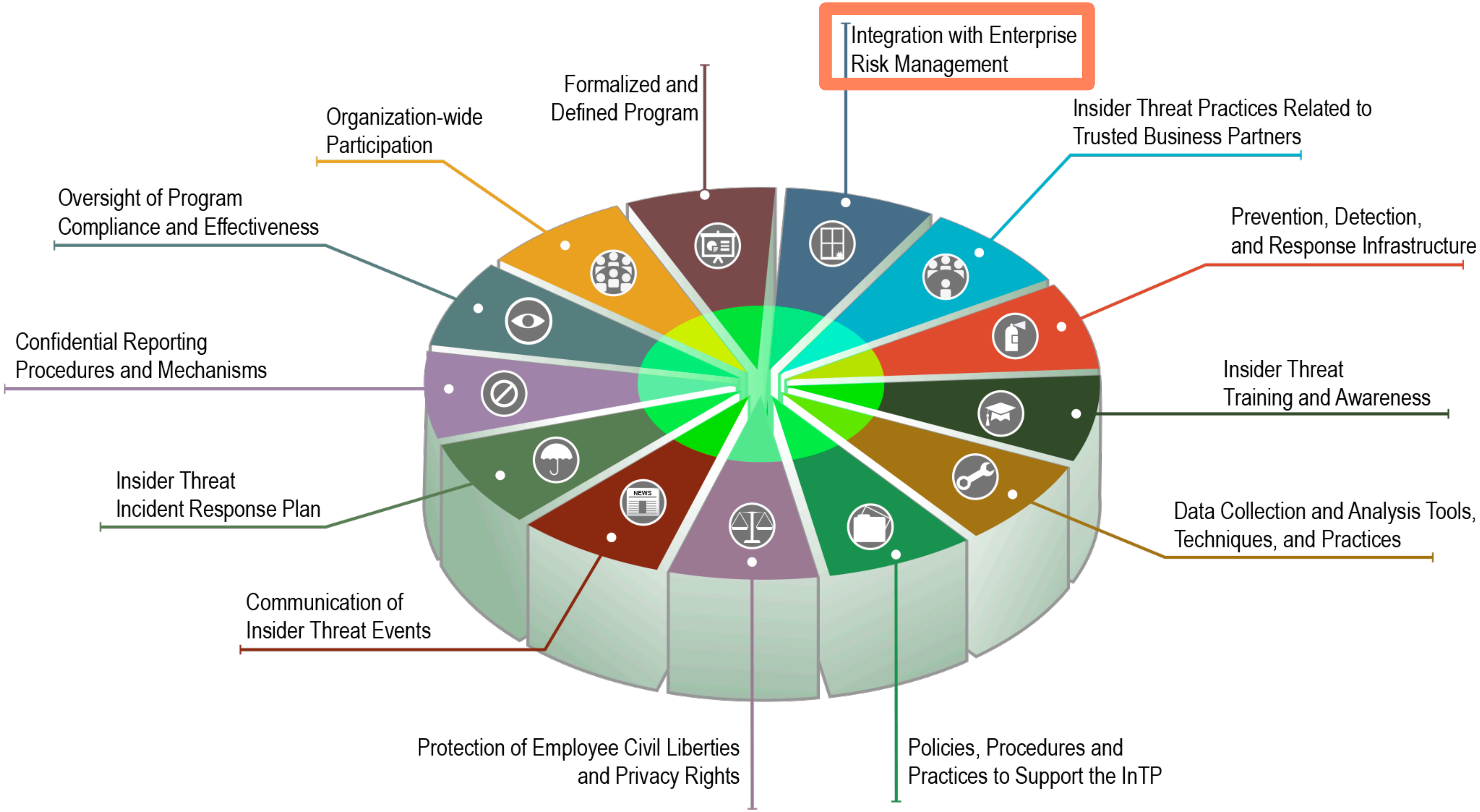
# The Goal for an Insider Threat Program…



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 InTP Key Components – It Starts With Risk Management


Integration with Enterprise Risk Management
Insider Threat Practices Related to Trusted Business Partners
Prevention, Detection, and Response Infrastructure
Insider Threat Training and Awareness
Data Collection and Analysis Tools, Techniques, and Practices
Policies, Procedures and Practices to Support the InTP
Protection of Employee Civil Liberties and Privacy Rights
Communication of Insider Threat Events
Insider Threat Incident Response Plan
Confidential Reporting Procedures and Mechanisms
Oversight of Program Compliance and Effectiveness
Organization-wide Participation
Formalized and Defined Program
NEWS

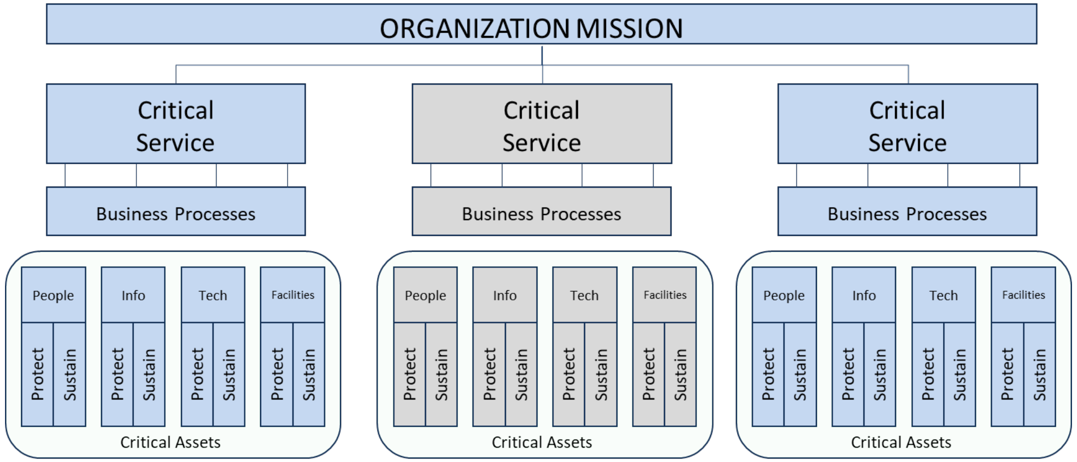
# Why Insider Risk Management?

- Ensures insider risks are managed consistently with other types of risk
- Allows the insider threat program to leverage existing resources
  - Avoids duplication of effort
  - Ensures the insider threat program is working with the best available information
- Enables precise definition of InTP scope and quantifiable goals

# What If No Risk Management Program Exists?

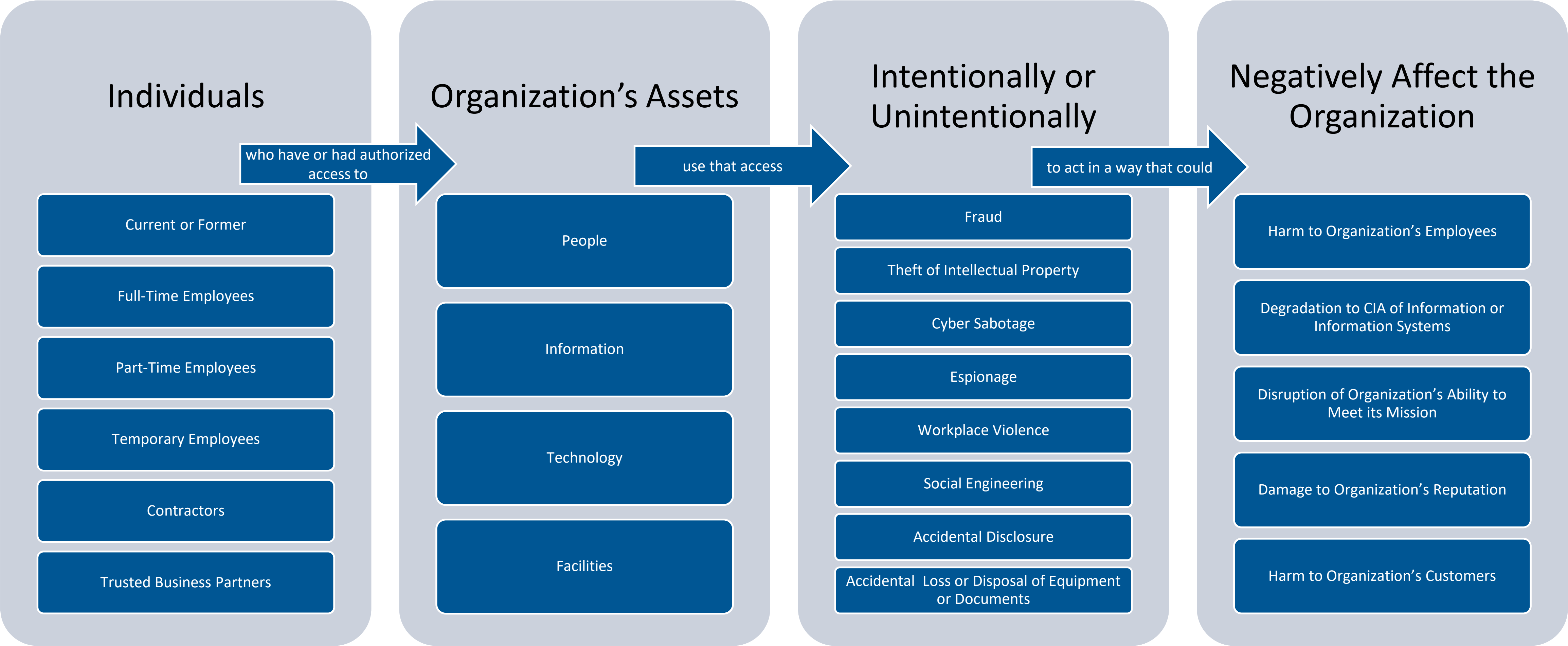
- A risk management-based approach is still recommended as the basis for the InTP.
  - The core activities of risk management are vital to the success of an InTP.
- Two options to consider:
  - The InTP can serve as the foundation for a broader enterprise risk management program.
  - An enterprise risk management program can be developed in parallel with the InTP.

# Critical Asset Identification



- Ask yourself:
  - What products or services do we provide?
  - What do we do in order to provide these services or products?
  - What assets do we use when performing these things?
  - What are the security requirements of these assets?
  - What is the value of these assets?

# Insider Threats to Critical Assets



## Individuals

who have or had authorized access to

- Current or Former
- Full-Time Employees
- Part-Time Employees
- Temporary Employees
- Contractors
- Trusted Business Partners

## Organization’s Assets

use that access

- People
- Information
- Technology
- Facilities

## Intentionally or Unintentionally

to act in a way that could

- Fraud
- Theft of Intellectual Property
- Cyber Sabotage
- Espionage
- Workplace Violence
- Social Engineering
- Accidental Disclosure
- Accidental  Loss or Disposal of Equipment or Documents

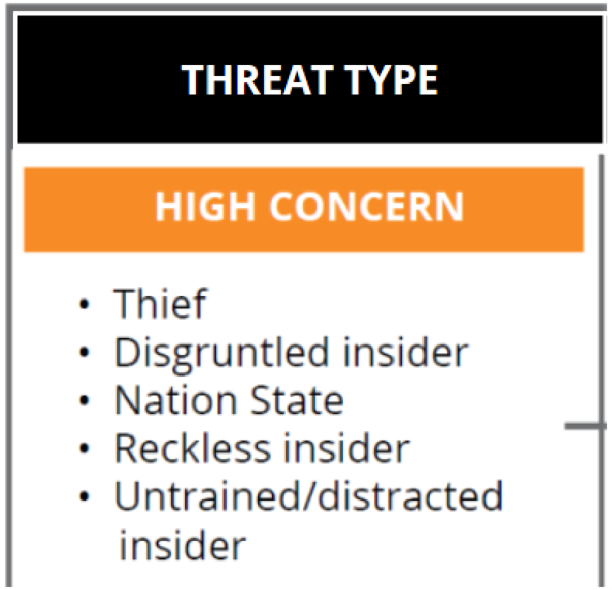
## Negatively Affect the Organization

- Harm to Organization’s Employees
- Degradation to CIA of Information or Information Systems
- Disruption of Organization’s Ability to Meet its Mission
- Damage to Organization’s Reputation
- Harm to Organization’s Customers

RSA Conference2022

# Holistic Insider Risk Management

# What Insider Threats Are Organizations Facing?



**THREAT TYPE**

**HIGH CONCERN**

- Thief
- Disgruntled insider
- Nation State
- Reckless insider
- Untrained/distracted insider

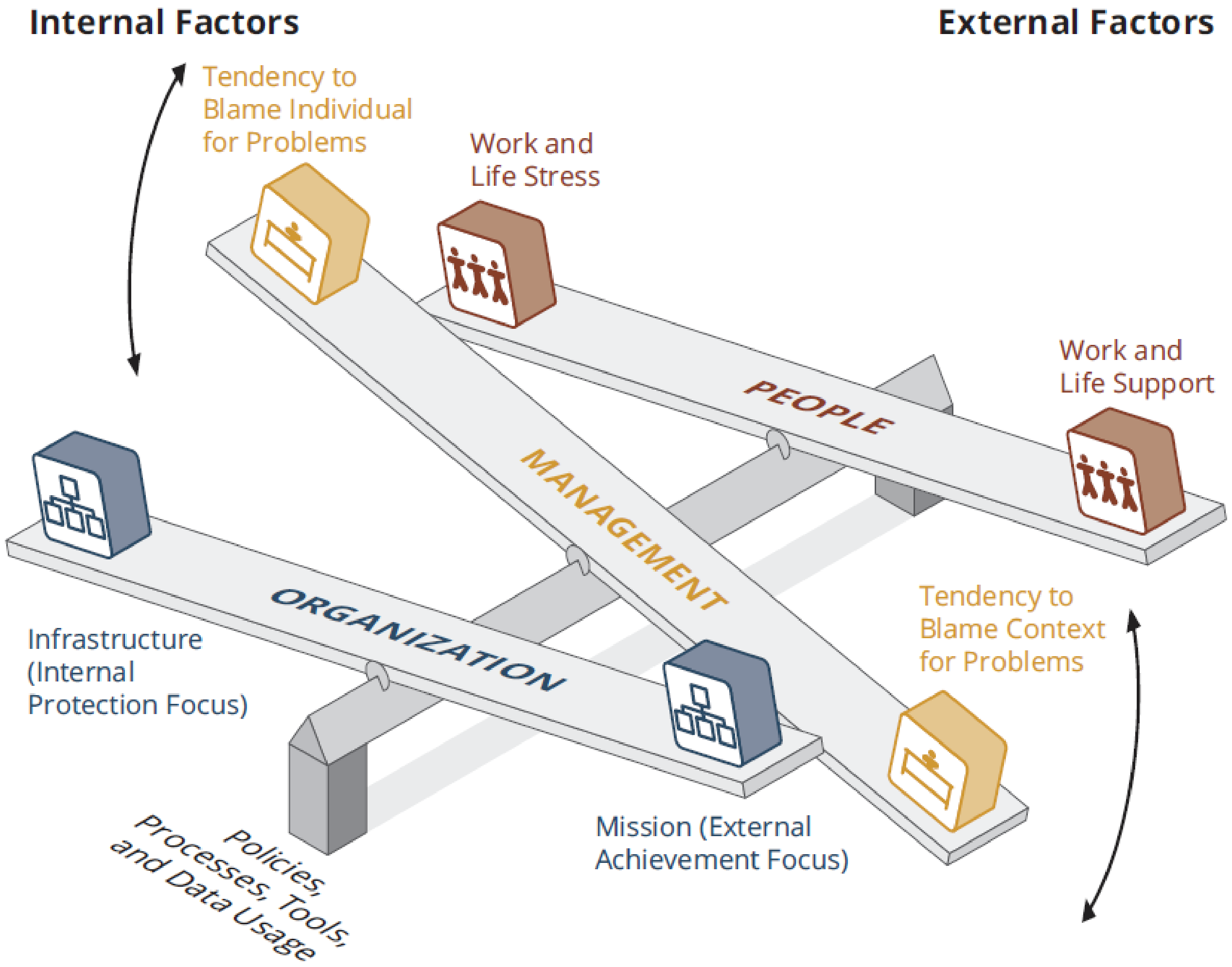
https://www.cylab.cmu.edu/_files/documents/irm-survey-results-20210331.7.pdf

# True Story: IT System Sabotage

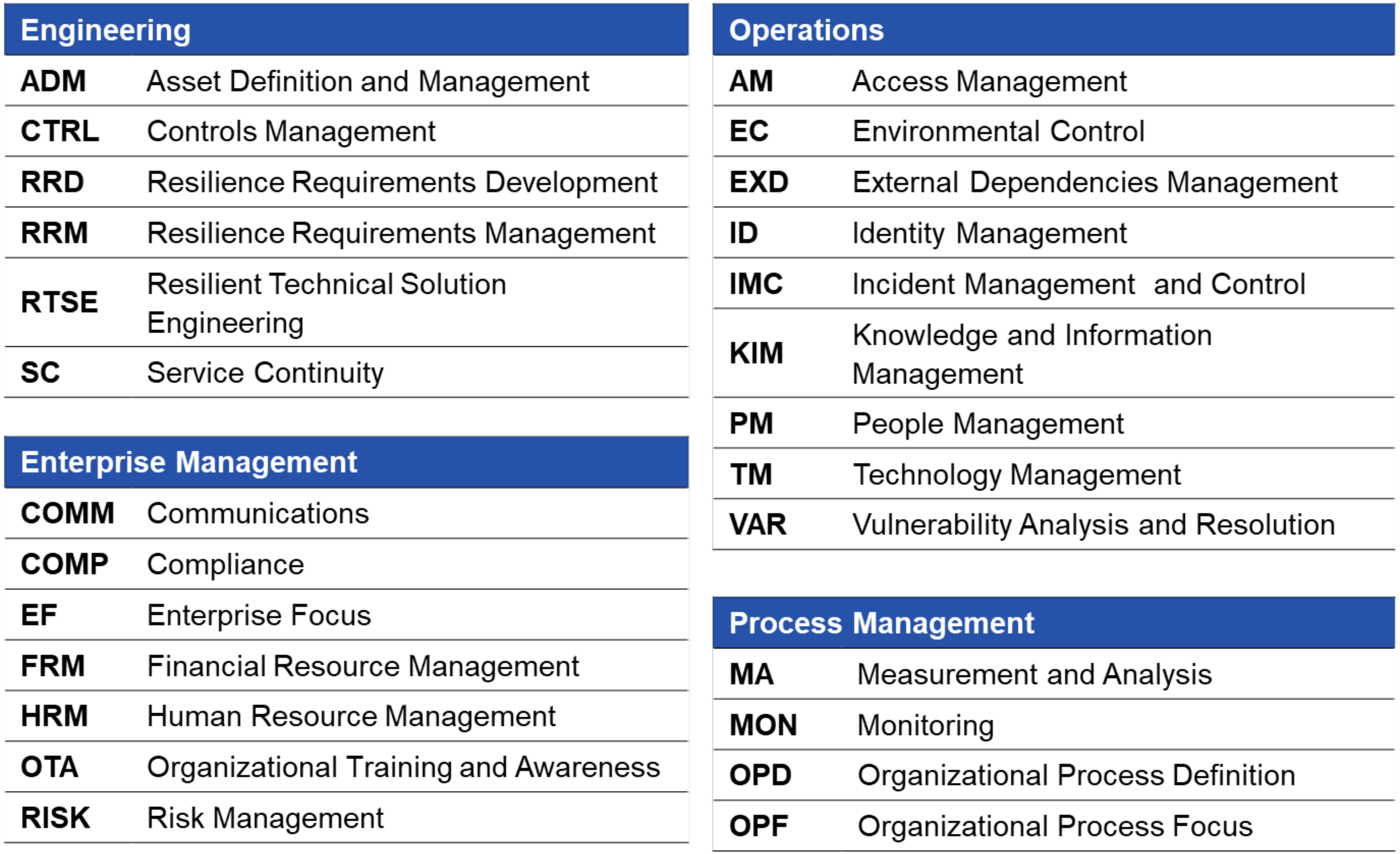
***911 emergency services disrupted for 4 major cities***

*Disgruntled former employee arrested and convicted for this deliberate act of sabotage.*

# A Balancing Act


Internal Factors
External Factors
Tendency to Blame Individual for Problems
Work and Life Stress
PEOPLE
Work and Life Support
MANAGEMENT
ORGANIZATION
Infrastructure (Internal Protection Focus)
Tendency to Blame Context for Problems
Mission (External Achievement Focus)
Policies, Processes, Tools, and Data Usage

# CERT Resilience Management Model (RMM)



| 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 |

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508084

# Where Organizations Traditionally Focus Insider Threat Mitigation Efforts

| 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 | |

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508084

# True Story: Theft of Intellectual Property

***Research scientist downloads 38,000 documents containing his company's trade secrets before going to work for a competitor…***

*Information was valued at $400 Million.*

# Where Insider Risk Management 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 | ☆ |

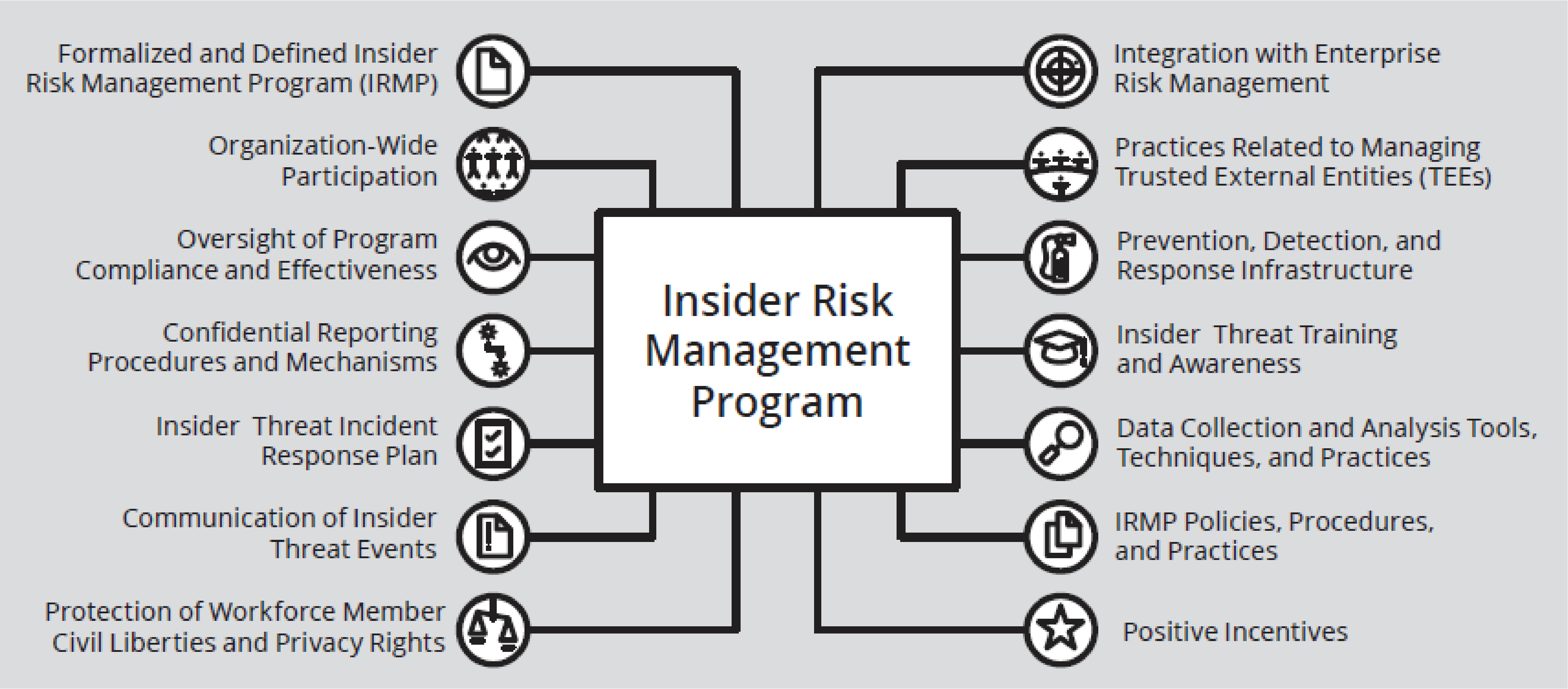
| Enterprise Management | | |
|---|---|---|
| **COMM** | Communications | ★ |
| **COMP** | Compliance | ☆ |
| **EF** | Enterprise Focus | ★ |
| **FRM** | Financial Resource Management | ★ |
| **HRM** | Human Resource Management | ★ |
| **OTA** | Organizational Training and Awareness | ★ |
| **RISK** | 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 | ☆ |

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508084

# A Holistic Insider Risk Management Program



Insider Risk Management Program

Formalized and Defined Insider Risk Management Program (IRMP)

Organization-Wide Participation

Oversight of Program Compliance and Effectiveness

Confidential Reporting Procedures and Mechanisms

Insider Threat Incident Response Plan

Communication of Insider Threat Events

Protection of Workforce Member Civil Liberties and Privacy Rights

Integration with Enterprise Risk Management

Practices Related to Managing Trusted External Entities (TEEs)

Prevention, Detection, and Response Infrastructure

Insider Threat Training and Awareness

Data Collection and Analysis Tools, Techniques, and Practices

IRMP Policies, Procedures, and Practices

Positive Incentives

# True Story: Fraud

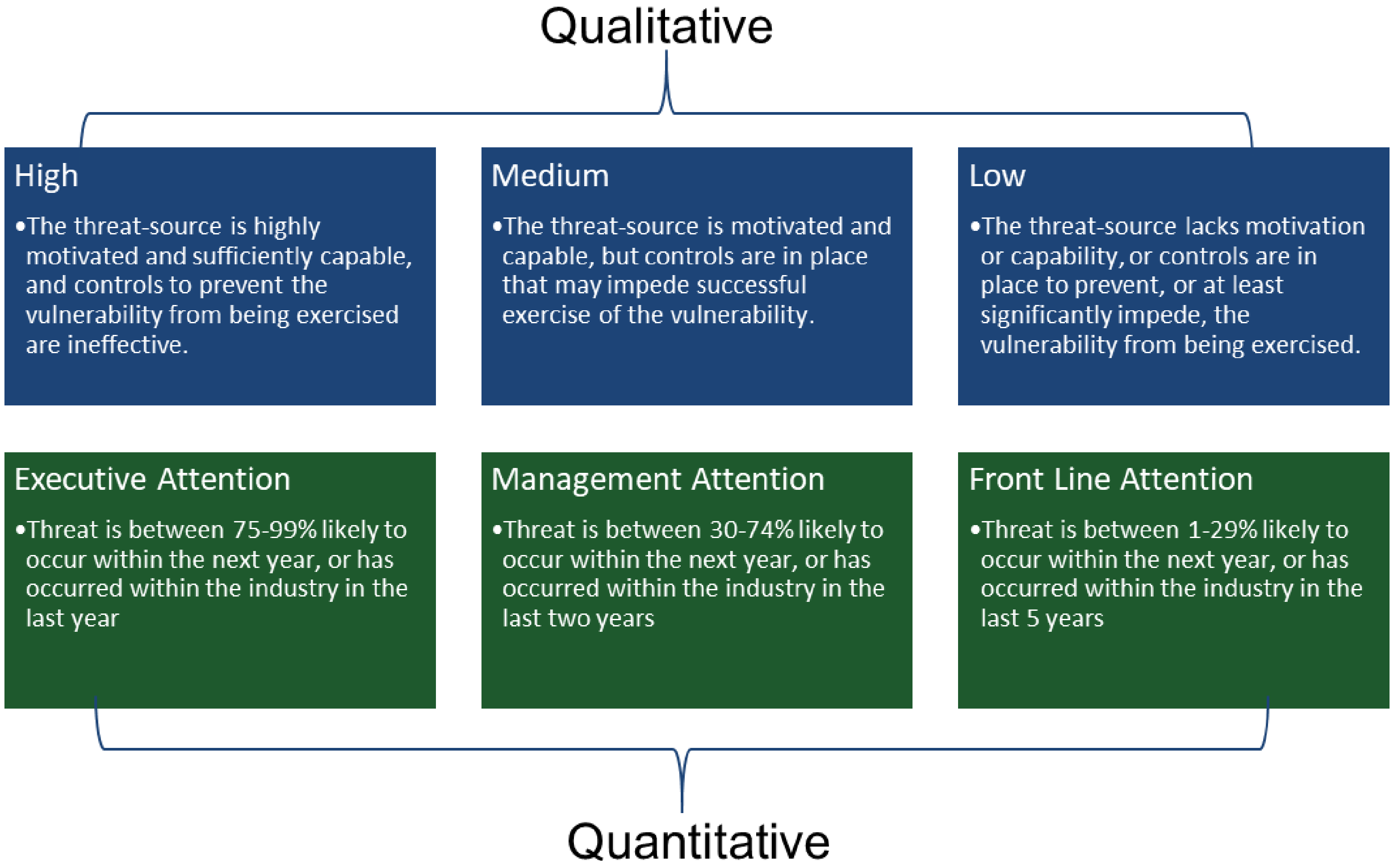
***An undercover agent who claims to be on the "No Fly list" buys a fake drivers license from a ring of DMV employees...***

*The identity theft ring consisted of 7 employees who sold more than 200 fake licenses for more than $1 Million.*

# Goal for an Insider Risk Management Program

- To reduce insider risks to critical assets to acceptable levels
- Struggling with formalizing and defining your program? Answer these questions:
  - What are “acceptable levels”?
    - How are you measuring risk?
  - What are your critical assets?
    - Who gets to decide, and do they change?

# Determining Likelihood



Qualitative

**High**

- The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.

**Medium**

- The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.

**Low**

- The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

**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**

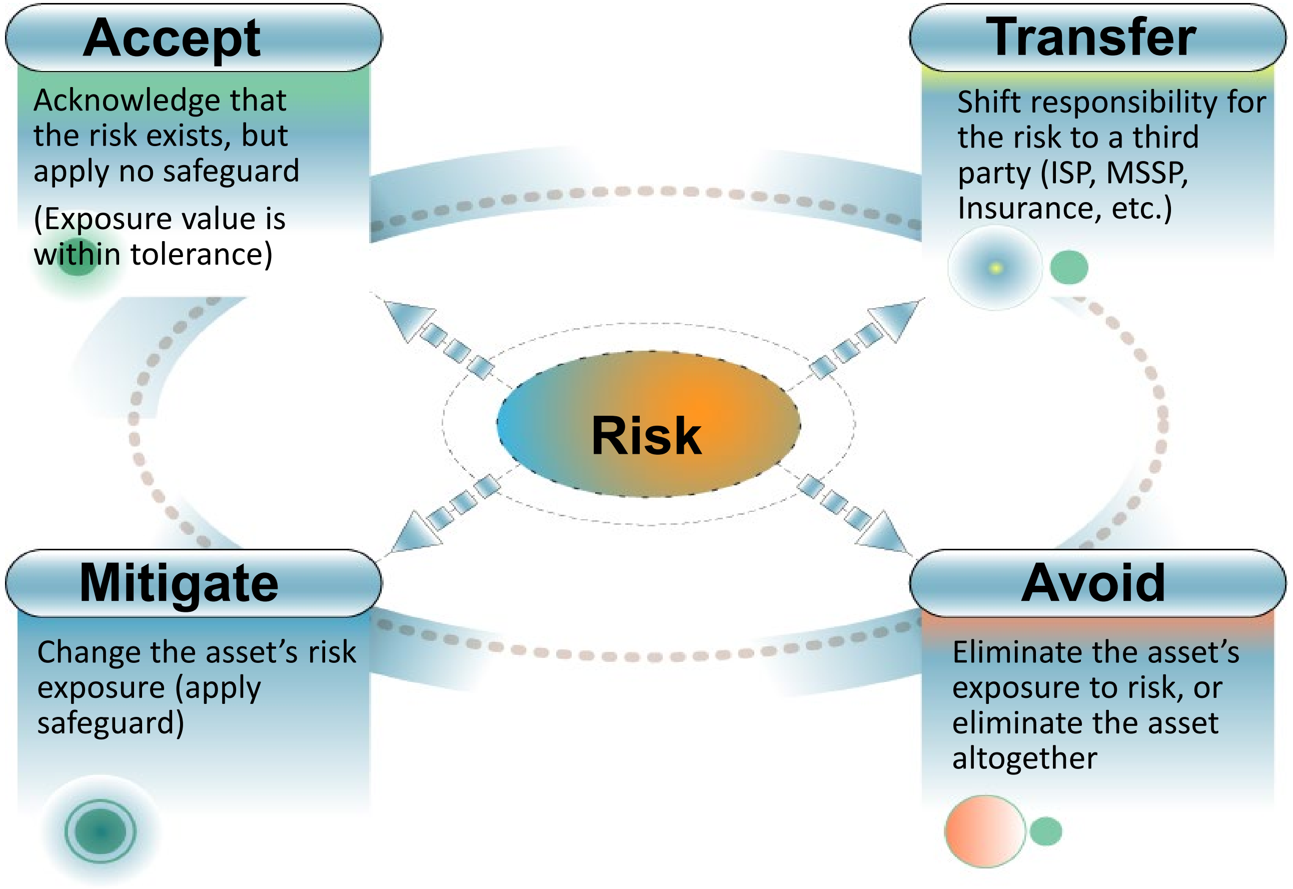
- Threat is between 30-74% likely to occur within the next year, or has occurred within the industry in the last two years

**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

Quantitative

# Managing Risks – 4 Choices

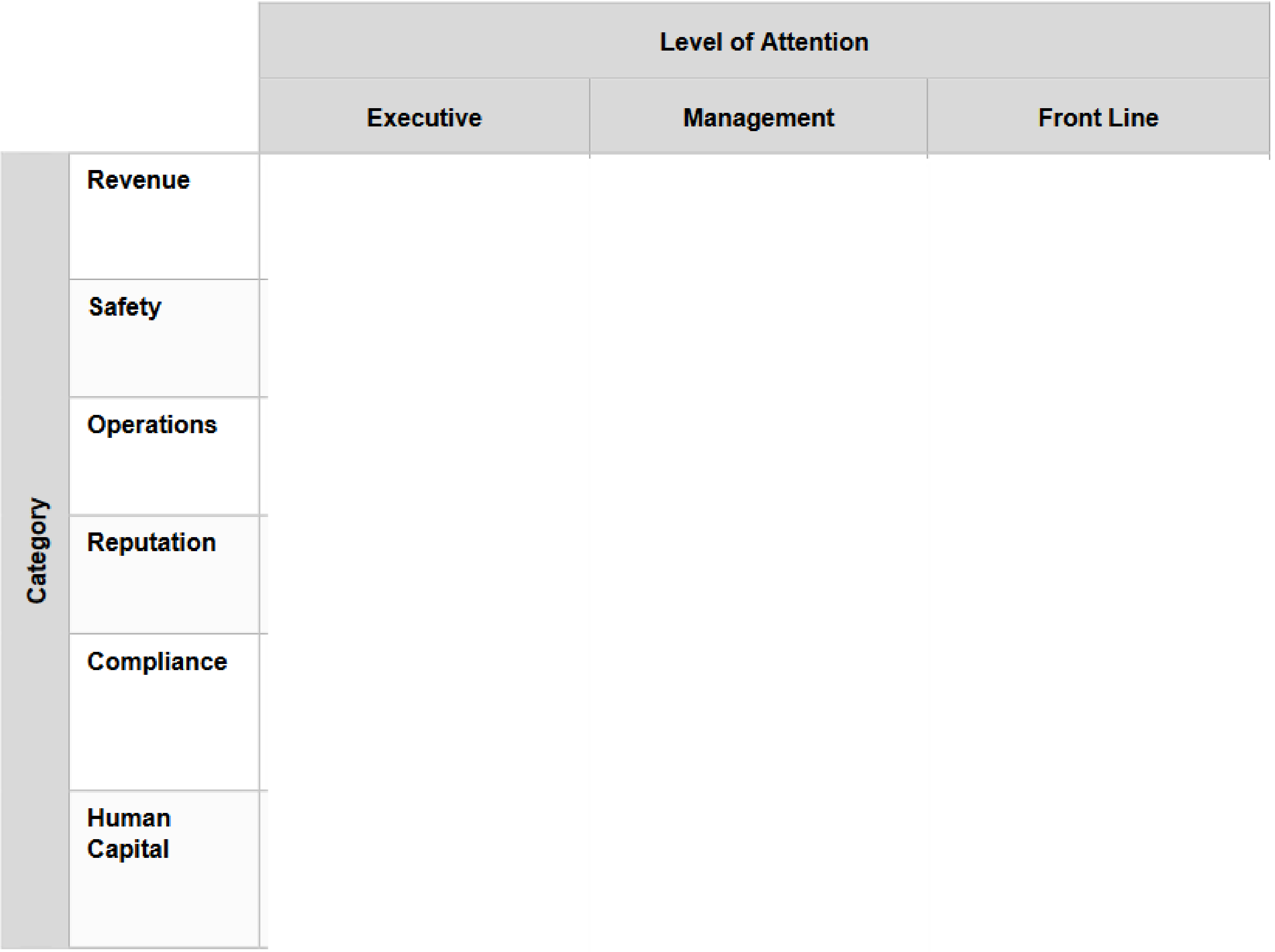


Accept
Acknowledge that the risk exists, but apply no safeguard
(Exposure value is within tolerance)
Transfer
Shift responsibility for the risk to a third party (ISP, MSSP, Insurance, etc.)
Risk
Mitigate
Change the asset's risk exposure (apply safeguard)
Avoid
Eliminate the asset's exposure to risk, or eliminate the asset altogether

# Insider Risk Appetite

# What Are “Acceptable Levels”? Establishing a Risk Appetite

## Impact

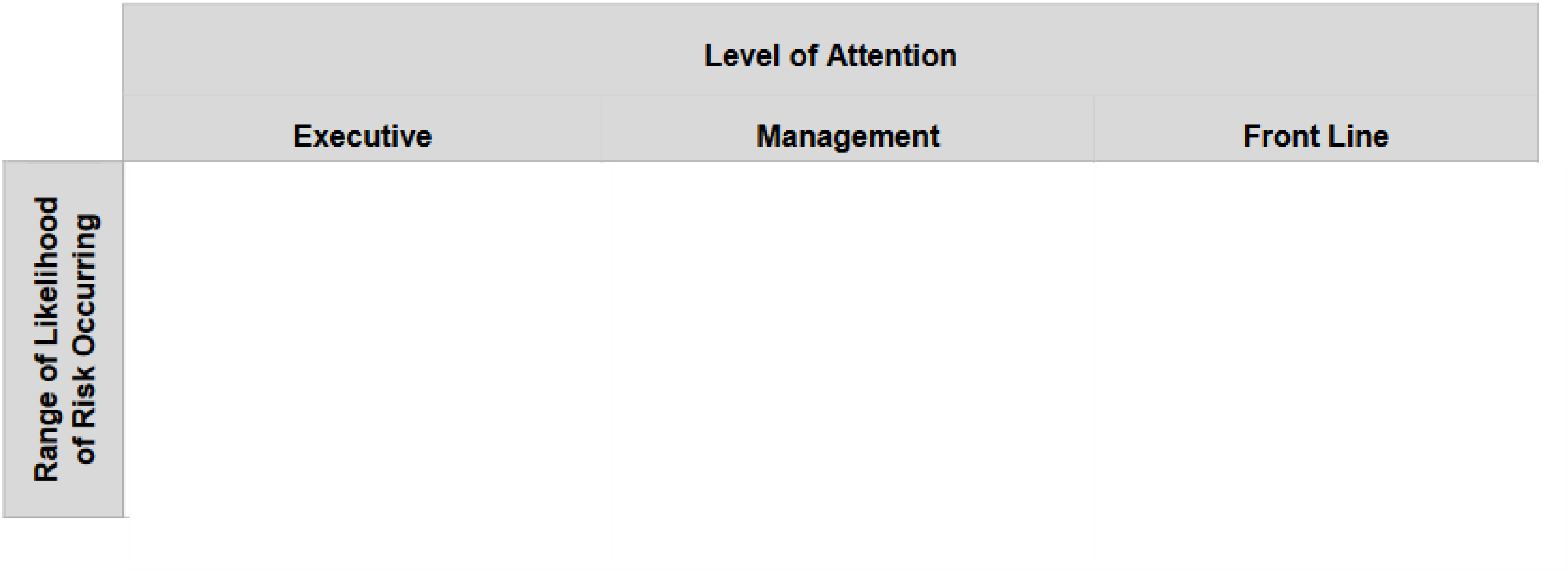


|  |  | Level of Attention |  |  |
|---|---|---|---|---|
|  |  | Executive | Management | Front Line |
| Category | Revenue |  |  |  |
|  | Safety |  |  |  |
|  | Operations |  |  |  |
|  | Reputation |  |  |  |
|  | Compliance |  |  |  |
|  | Human Capital |  |  |  |

https://resources.sei.cmu.edu/asset_files/TechnicalNote/2020_004_001_644641.pdf

# What Are "Acceptable Levels"? Establishing a Risk Appetite

## Likelihood

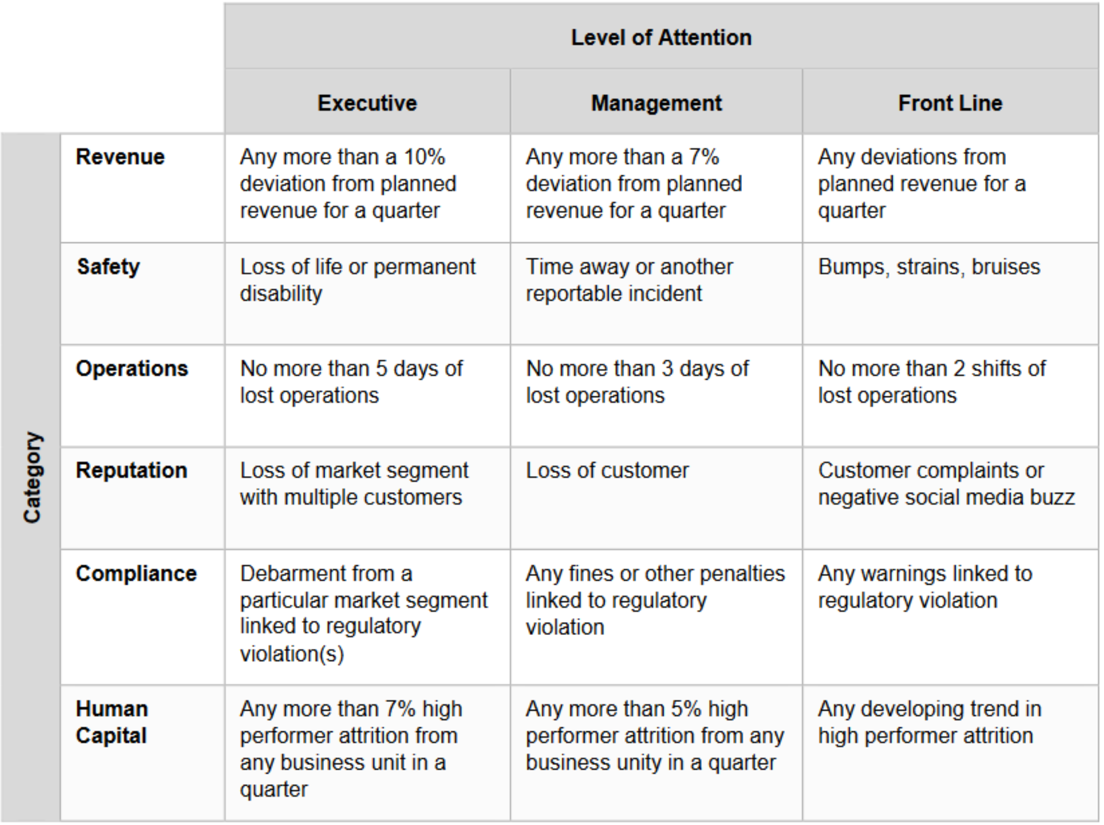


| | Level of Attention | | |
|---|---|---|---|
| | Executive | Management | Front Line |
| Range of Likelihood of Risk Occurring | | | |

https://resources.sei.cmu.edu/asset_files/TechnicalNote/2020_004_001_644641.pdf

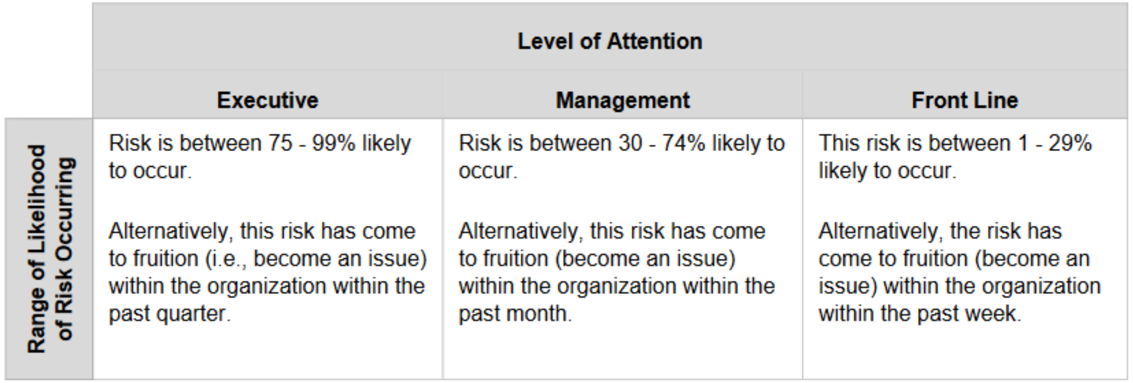
# What Are “Acceptable Levels”? Establishing a Risk Appetite

## Impact



| | | Level of Attention | | |
|---|---|---|---|---|
| | | **Executive** | **Management** | **Front Line** |
| Category | **Revenue** | Any more than a 10% deviation from planned revenue for a quarter | Any more than a 7% deviation from planned revenue for a quarter | Any deviations from planned revenue for a quarter |
| | **Safety** | Loss of life or permanent disability | Time away or another reportable incident | Bumps, strains, bruises |
| | **Operations** | No more than 5 days of lost operations | No more than 3 days of lost operations | No more than 2 shifts of lost operations |
| | **Reputation** | Loss of market segment with multiple customers | Loss of customer | Customer complaints or negative social media buzz |
| | **Compliance** | Debarment from a particular market segment linked to regulatory violation(s) | Any fines or other penalties linked to regulatory violation | Any warnings linked to regulatory violation |
| | **Human Capital** | Any more than 7% high performer attrition from any business unit in a quarter | Any more than 5% high performer attrition from any business unity in a quarter | Any developing trend in high performer attrition |

## Likelihood



| | Level of Attention | | |
|---|---|---|---|
| | **Executive** | **Management** | **Front Line** |
| **Range of Likelihood of Risk Occurring** | Risk is between 75 - 99% likely to occur.<br>Alternatively, this risk has come to fruition (i.e., become an issue) within the organization within the past quarter. | Risk is between 30 - 74% likely to occur.<br>Alternatively, this risk has come to fruition (become an issue) within the organization within the past month. | This risk is between 1 - 29% likely to occur.<br>Alternatively, the risk has come to fruition (become an issue) within the organization within the past week. |

https://resources.sei.cmu.edu/asset_files/TechnicalNote/2020_004_001_644641.pdf

# Apply What You Have Learned Today

- Next week you should:
  - Identify how risk appetites are described within your organization
- In the first three months following this presentation you should:
  - Establish a method for measuring current security posture against insider risks to critical assets that aligns with risk appetite statements
- Within six months you should:
  - Describe the performance of your insider management program in the context of your newly-established risk tolerances

# For More Information

- CERT Common Sense Guide to Managing Insider Risk
- Insider Risk Management Program Evaluation Assessment Instrument
- Insider Risk Management Program Building: Results from a Survey of Practitioners
- Advancing Risk Management Capability Using the OCTAVE FORTE Process
- cert.org/insider-threat