Risk and Resilience: Considerations for Information Security Risk Assessment and Management

Julia Allen and Jim Cebula

CERT Program

Software Engineering Institute

Session ID: GRC-202
Session Classification: Intermediate

RSACONFERENCE2011

Objectives

Get you talking a common language about risk concepts

Introduce you to the CERT Resilience Management Model

Start you thinking about these concepts In your organization

Some Questions to Consider

- Performance or compliance measures?
- Are you measuring at all?
- Reactive or proactive?
- Can you sustain your performance under stress? How would you know?
- Do you have a process to *manage* your monitoring efforts?
- What is your organization's risk tolerance?
- Who is responsible for accepting risk? Is there a process?
- What risks has the organization accepted?

Words Matter. . .

Vulnerability

Condition

Exposure

Impact

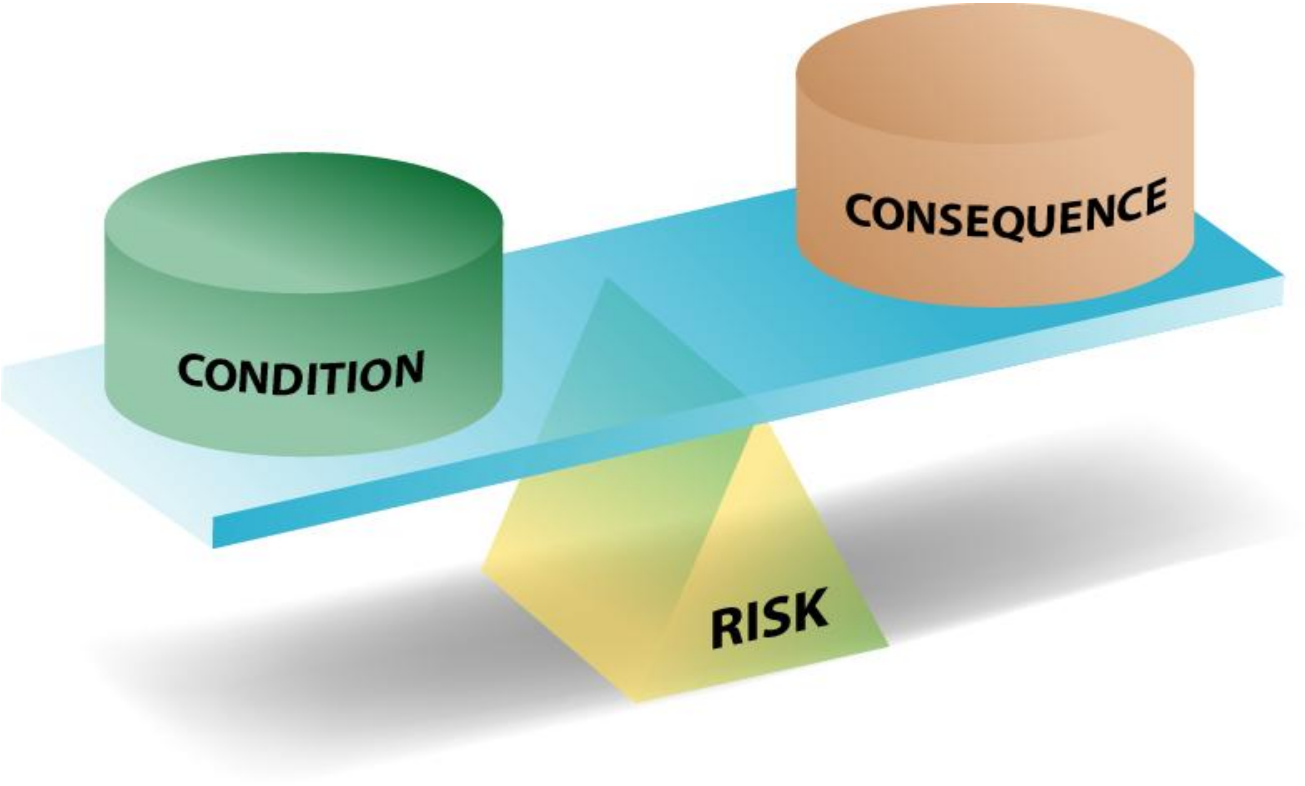
Threat

Consequence

Weakness

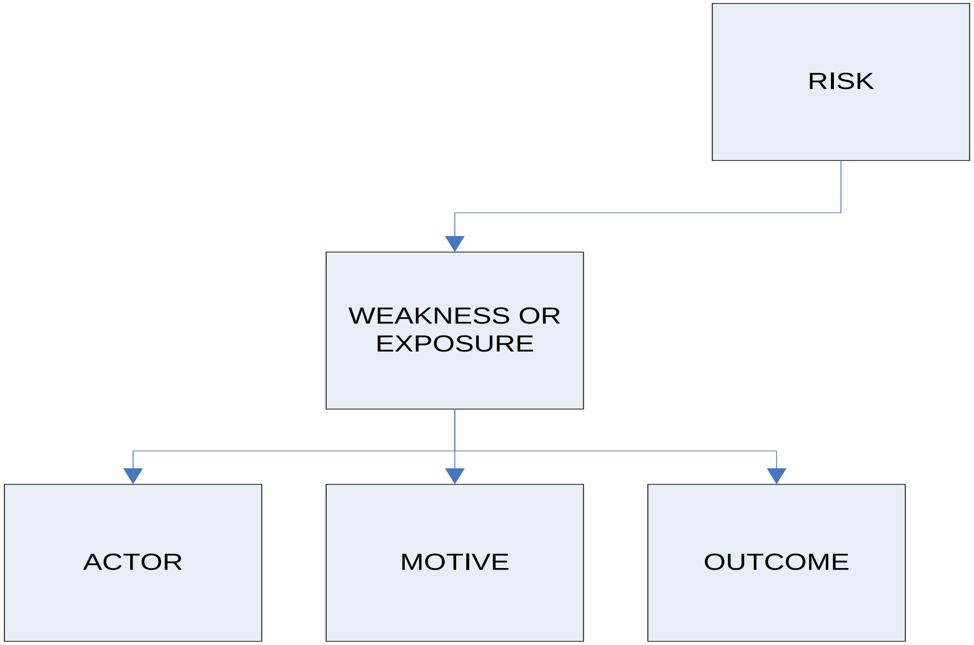
Elements of Risk

The Basic Risk Equation

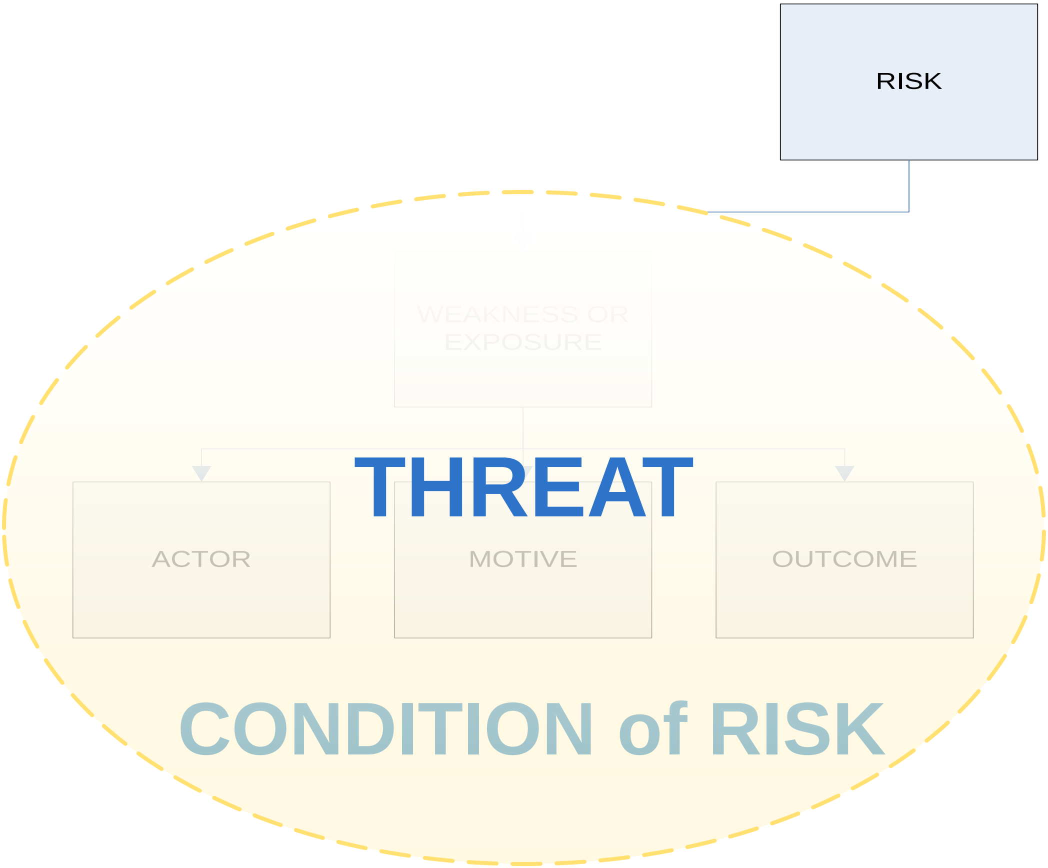


RISK = CONDITION + CONSEQUENCE

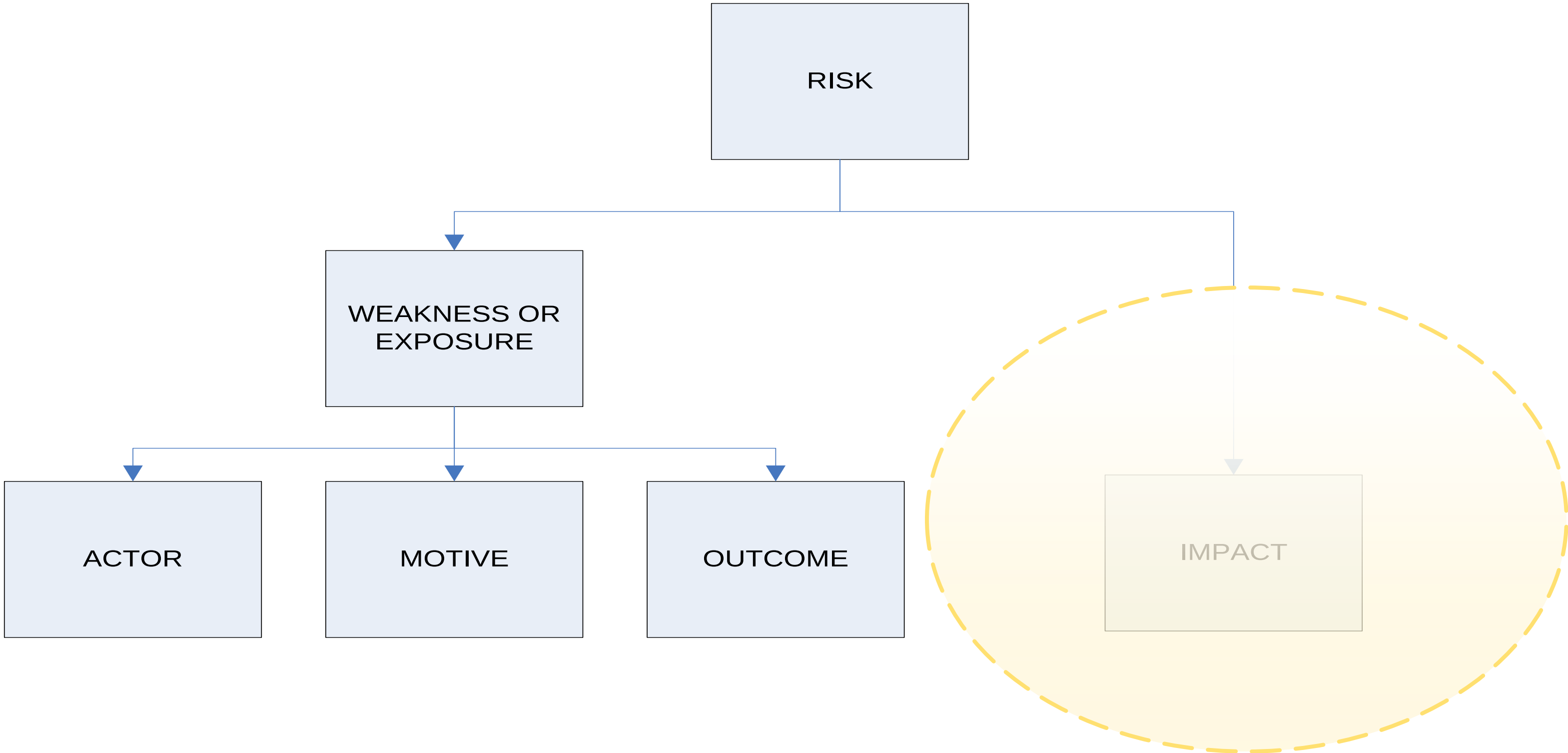
Assembling the Risk Elements



Assembling the Risk Elements



Positioning "Impact" in Risk



CONSEQUENCE of RISK

Outcome vs. Consequences

Outcome - unwanted or unintended results of an actor with a motive exploiting a weakness, exposure, or vulnerability

Examples:

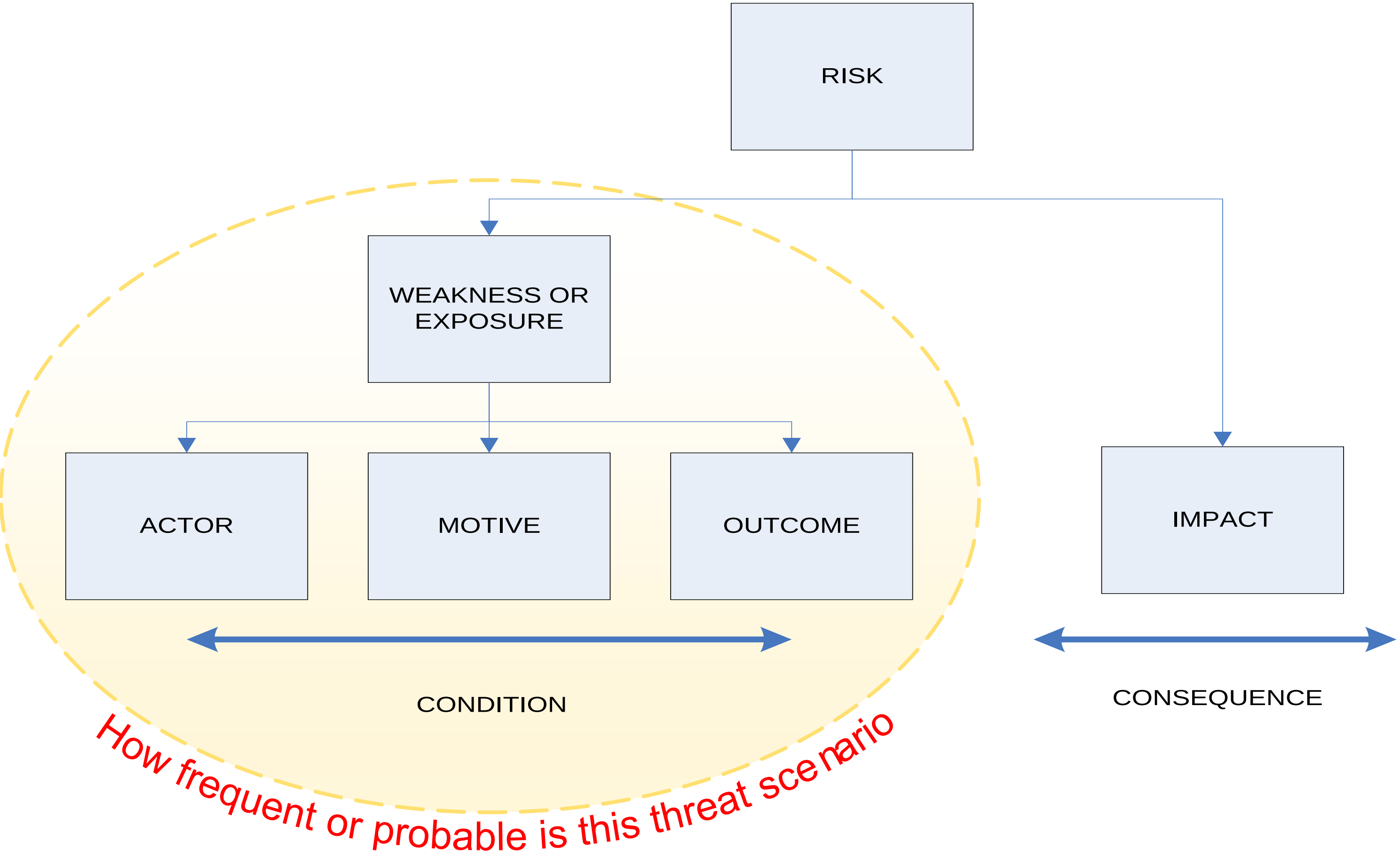
- **Access to email or critical systems is denied**
- **Network is slow; users can't access Internet**
- **Customers can't place orders on web site**
- **Remote sensors shut down on gas valves causing explosion**

Consequence refers to the impact on a person or organization as a result of the exploitation

Examples:

- **Loss of $50,000 in revenue per hour**
- **Productivity loss of 45% resulting in $500,000 of rework**
- **Reputational damage due to news coverage**
- **Fine of $1,000,000**
- **Loss of life for 20 employees**

Adding Uncertainty



RISK

WEAKNESS OR EXPOSURE

ACTOR

MOTIVE

OUTCOME

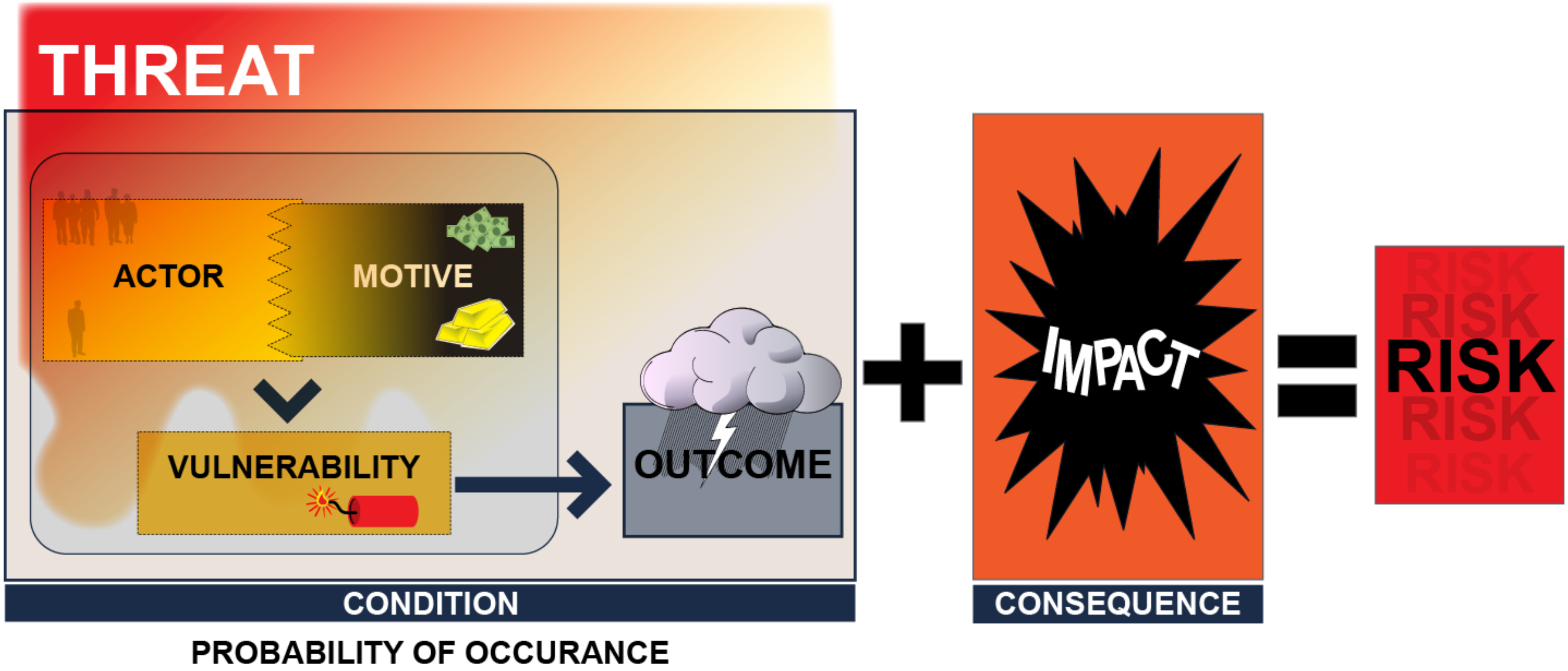
IMPACT

CONDITION

CONSEQUENCE

How frequent or probable is this threat scenario

It All Adds Up To …



Operational Risk

Basic Types of Risk

- Four generally accepted types of risk:
  1. Hazard
  2. Financial
  3. Operational
  4. Strategic
- Boundaries can overlap—for example:
  - Hazard risk (fire, flood) can be a component of operational risk.
  - Strategic risk can include financial risks related to strategy decisions.

Operational Risk

- A form of hazard risk affecting day-to-day business operations
- The potential failure to achieve mission objectives
- Inclusive of “security risks”

Actions of people

```
A fatal exception
000059F8. The curr

* Press any key to
* Press CTRL+ALT+D
  lose any unsaved
```

Systems & technology failures

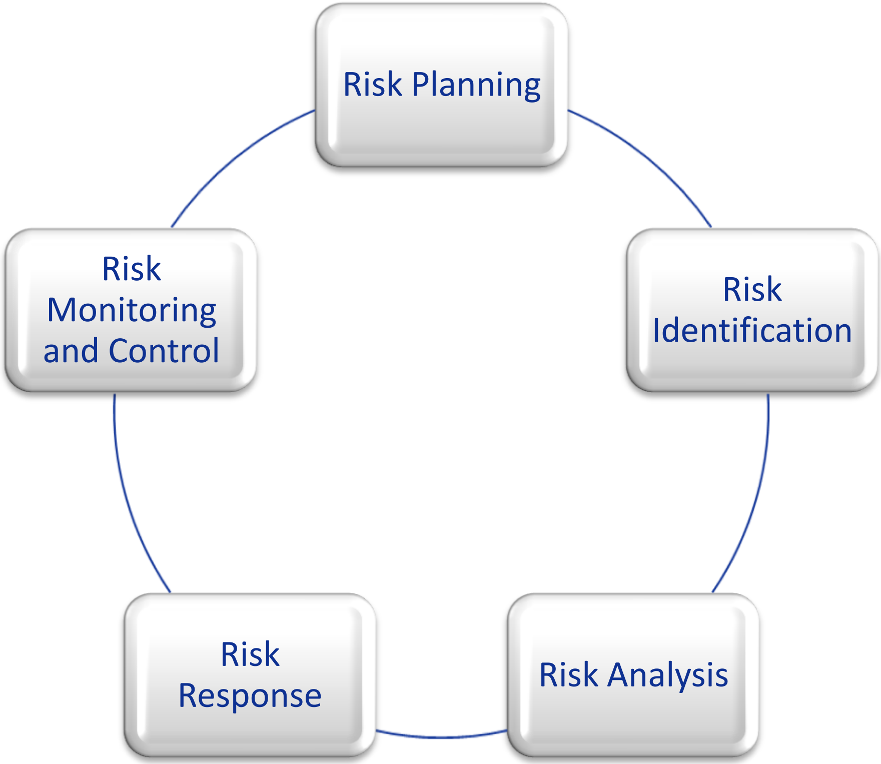
Failed internal processes

External events

Operational Risk Management

Operational Risk Management

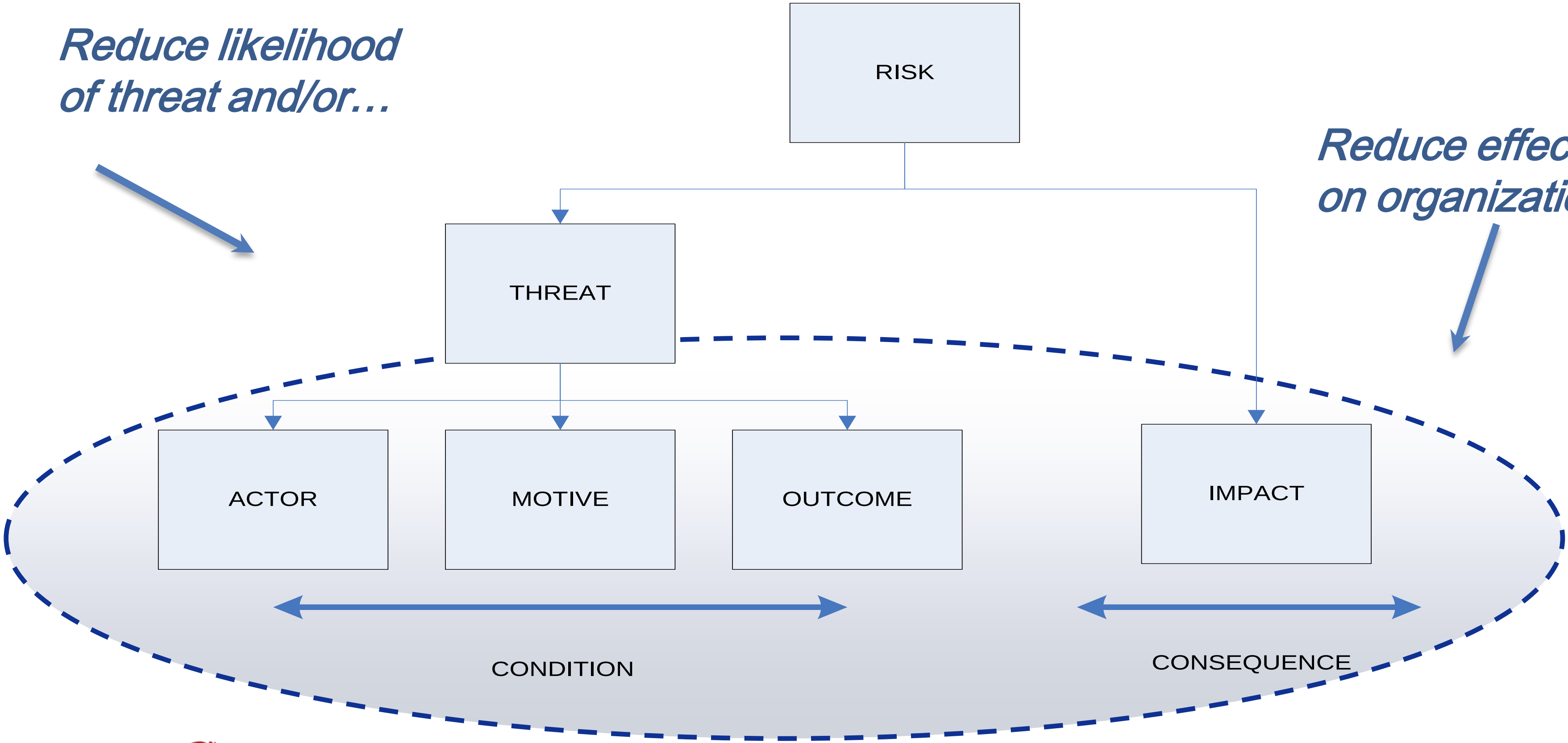
A continuous cycle of operational risk management activities



Risk Avoidance vs. Risk Mitigation

Reduce likelihood of threat and/or…

Reduce effects on organization



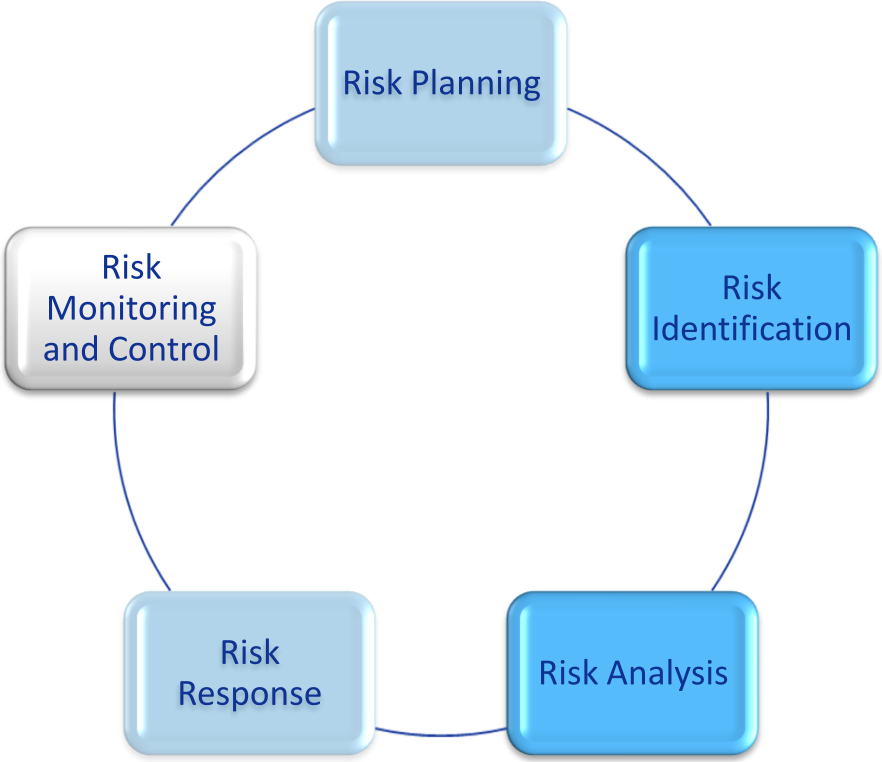
Risk Monitoring and Control

- Process of
  - identifying, analyzing, and planning for new risks
  - monitoring existing risks and their response strategies (for effectiveness)
  - monitoring the status of residual risks
  - identifying and implementing triggers to determine when risks should be reviewed, new risk identification should occur, etc.

- Once a risk response has been implemented, **risks do not go away!**

Where Does Risk Assessment Fit?

- Risk assessment includes:
  - Risk planning
  - Risk identification
  - Risk analysis
  - Risk response
- It is the "diagnostic" part of the continuous risk management cycle



Vulnerability vs. Risk Assessment

- **Vulnerability assessment** is a means to identify threats: weaknesses, exposures, and vulnerabilities
- Examples:
  - Running automated assessment tools
  - Doing penetration tests

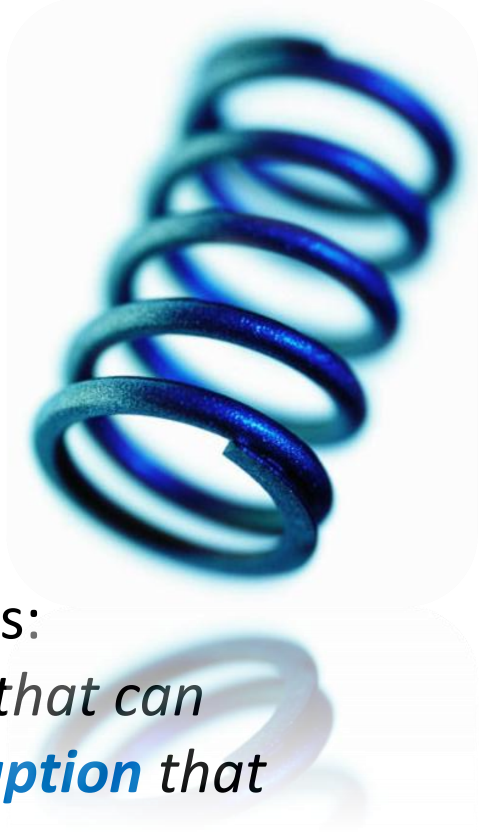
- **Risk assessment** is a process of identifying risks relative to threat; includes probability, impact, and consequence

Vulnerability assessment is NOT equal to risk assessment.

Risk and Resilience

Resilience Defined

- The physical property of a material that can return to its original shape or position after deformation that does not exceed its elastic limit
  [wordnet.princeton.edu]



Parsed in organizational (and operational) terms:

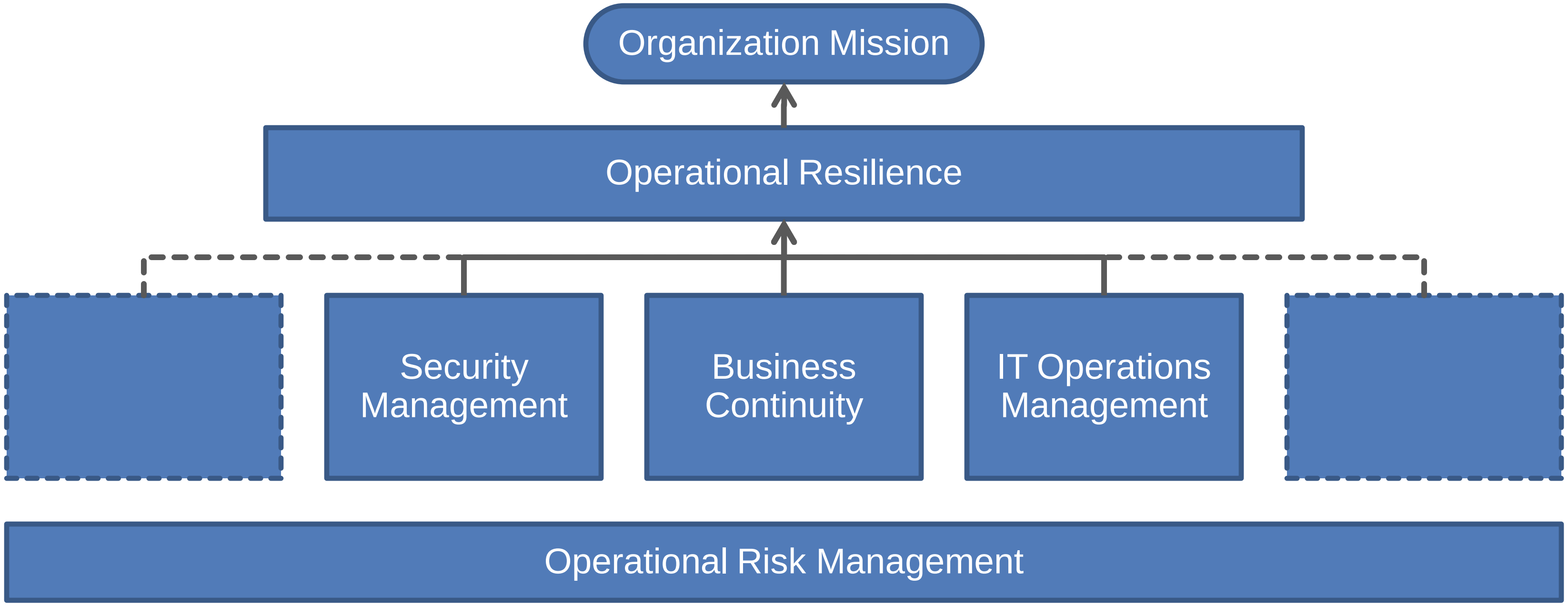
> *The **emergent** property of an **organization** that can **continue to carry out its mission** after **disruption** that does not exceed its **operational** limit*

Where does the **disruption** come from? Realized risk.

Operational Risk and Operational Resilience

- Known risk is addressed before it becomes disruptive.
- Organizations can more easily predict the performance of business services under uncertain conditions (i.e., unknown risks).
- An operationally-resilient service
  - Can meet its mission under adverse circumstances (times of stress, within some limit)
  - AND return to normal when the adversity (stress) is eliminated

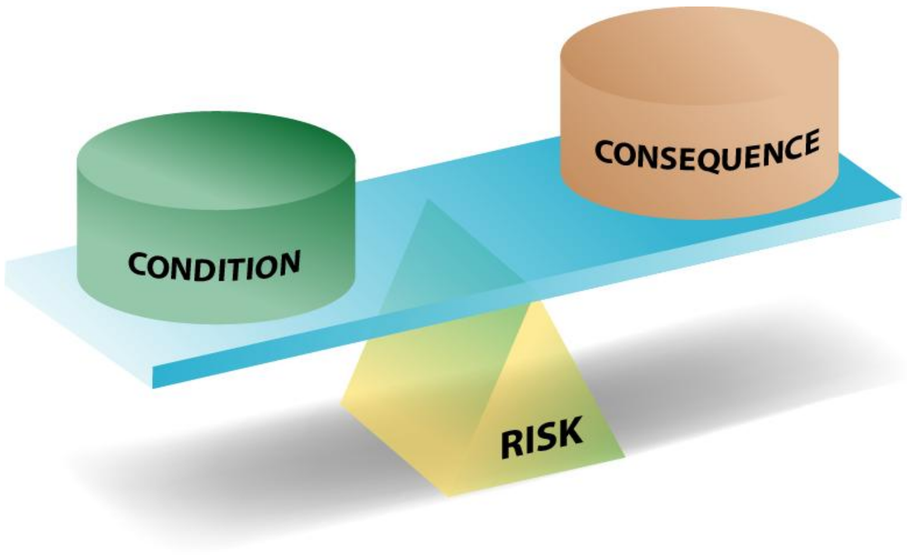
Operational Resilience and Convergence



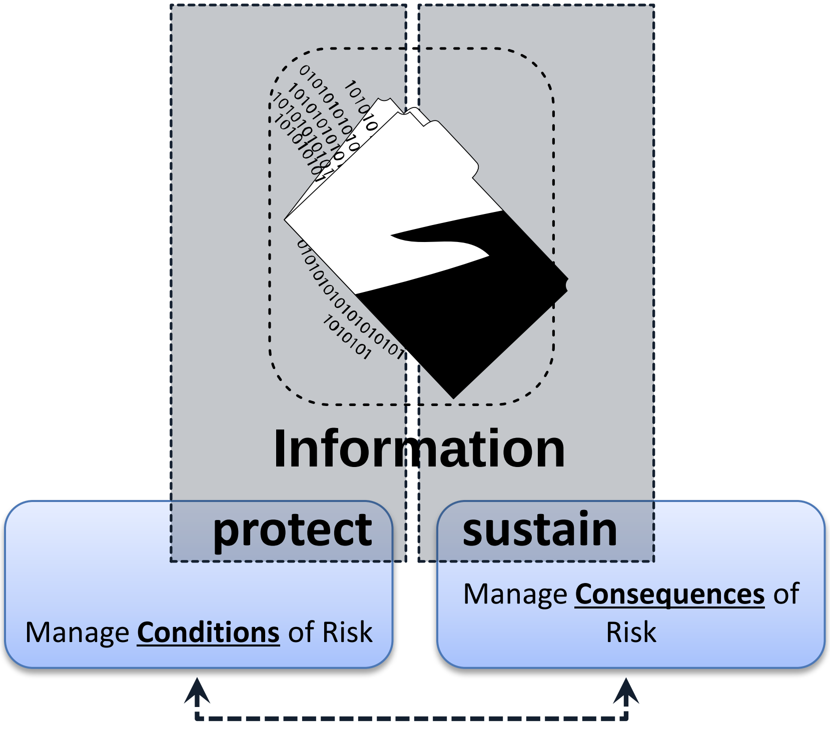
- Convergence directly affects the level of operational resilience.
- Level of operational resilience affects the ability to meet organizational mission.

Protection, Sustainability, and Risk

Basic risk equation



Protection & sustainability



Manage **Conditions** of Risk

Manage **Consequences** of Risk

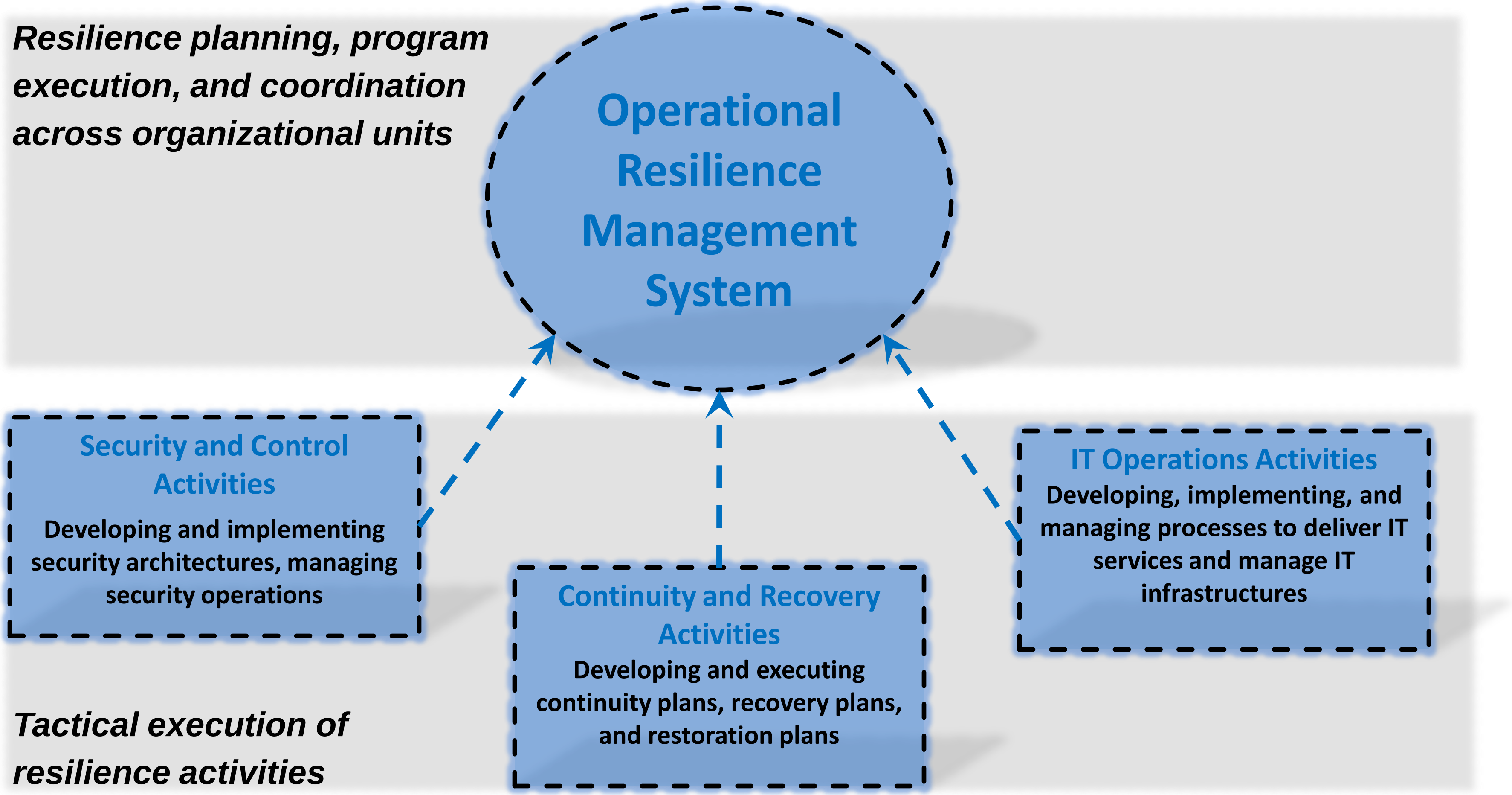
The CERT
Resilience Management Model
(CERT-RMM)

What is CERT-RMM?

- *CERT-RMM is a maturity model for managing and improving operational resilience.*

- Guides implementation and management of operational resilience activities
- Converges key operational risk management activities: security, BC/DR, and IT operations
- Defines maturity through capability levels *(like CMMI)*
- Improves confidence in how an organization responds in times of operational stress

Layers of Resilience Activities



Resilience planning, program execution, and coordination across organizational units

Operational Resilience Management System

Security and Control Activities

Developing and implementing security architectures, managing security operations

Continuity and Recovery Activities

Developing and executing continuity plans, recovery plans, and restoration plans

IT Operations Activities

Developing, implementing, and managing processes to deliver IT services and manage IT infrastructures

Tactical execution of resilience activities

Imperatives for Building CERT-RMM

Tech reliance

Global economy

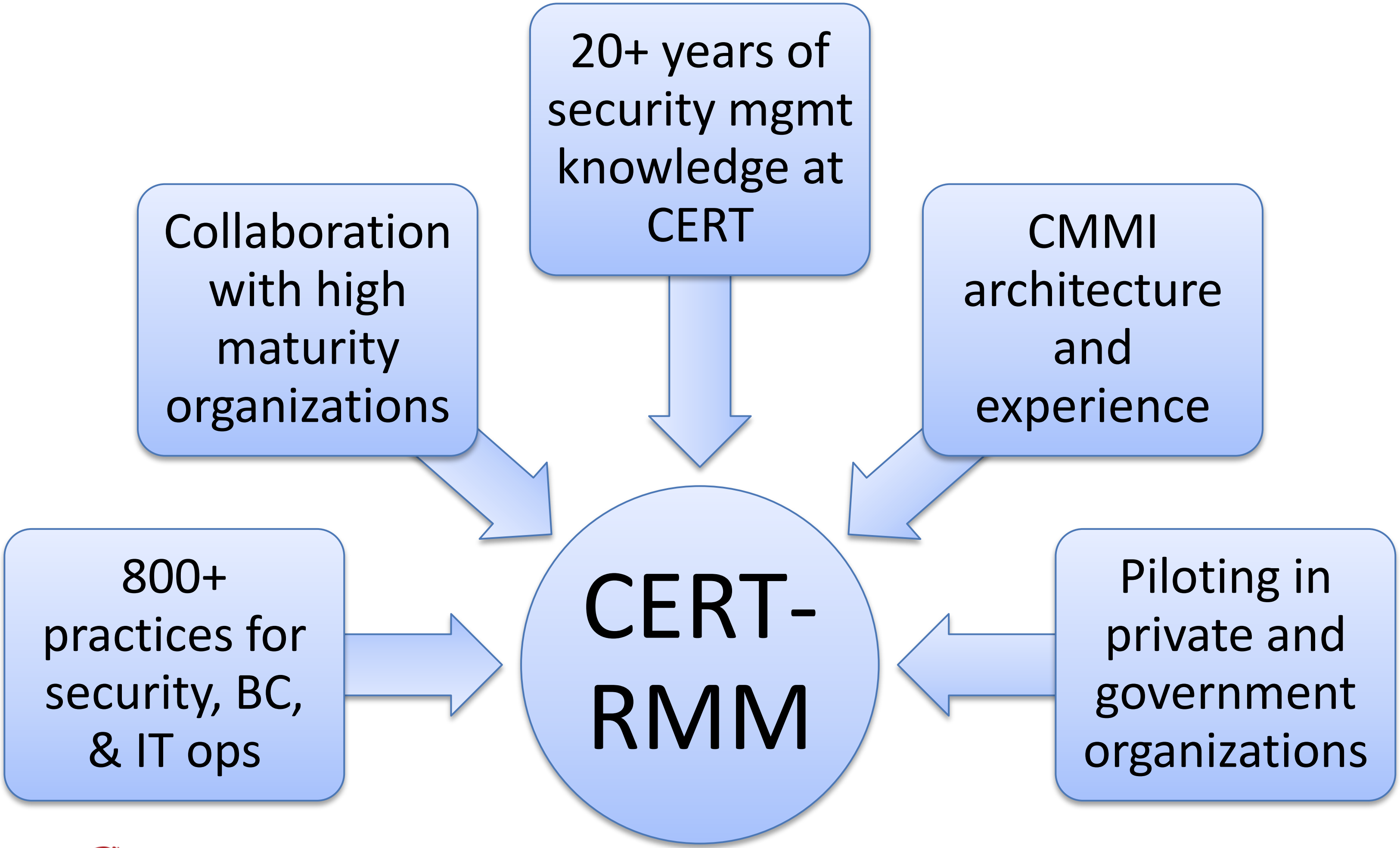
Open boundaries

Complexity

Cultural shifts

- Increasingly complex operational environments where traditional approaches are failing
- Siloed nature of operational risk activities; a lack of convergence
- Lack of common language or taxonomy
- Overreliance on technical approaches
- Lack of means to measure managerial competency
- **Inability to confidently predict outcomes, behaviors, and performance under times of stress**

CERT-RMM Background



20+ years of security mgmt knowledge at CERT

Collaboration with high maturity organizations

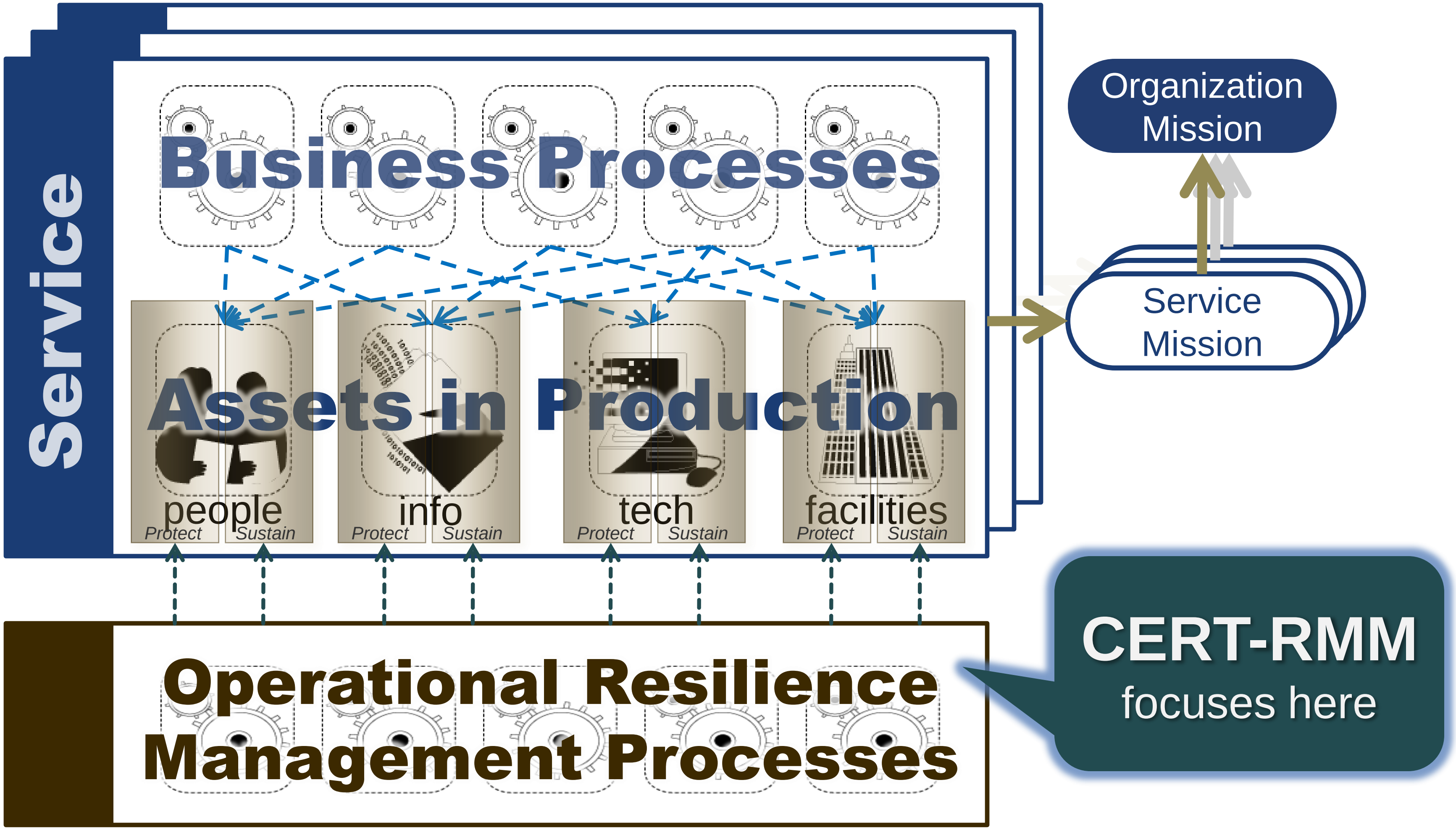
CMMI architecture and experience

800+ practices for security, BC, & IT ops

CERT-RMM

Piloting in private and government organizations

Organizational Context



CERT-RMM: 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 & Awareness
RISK	Risk Management

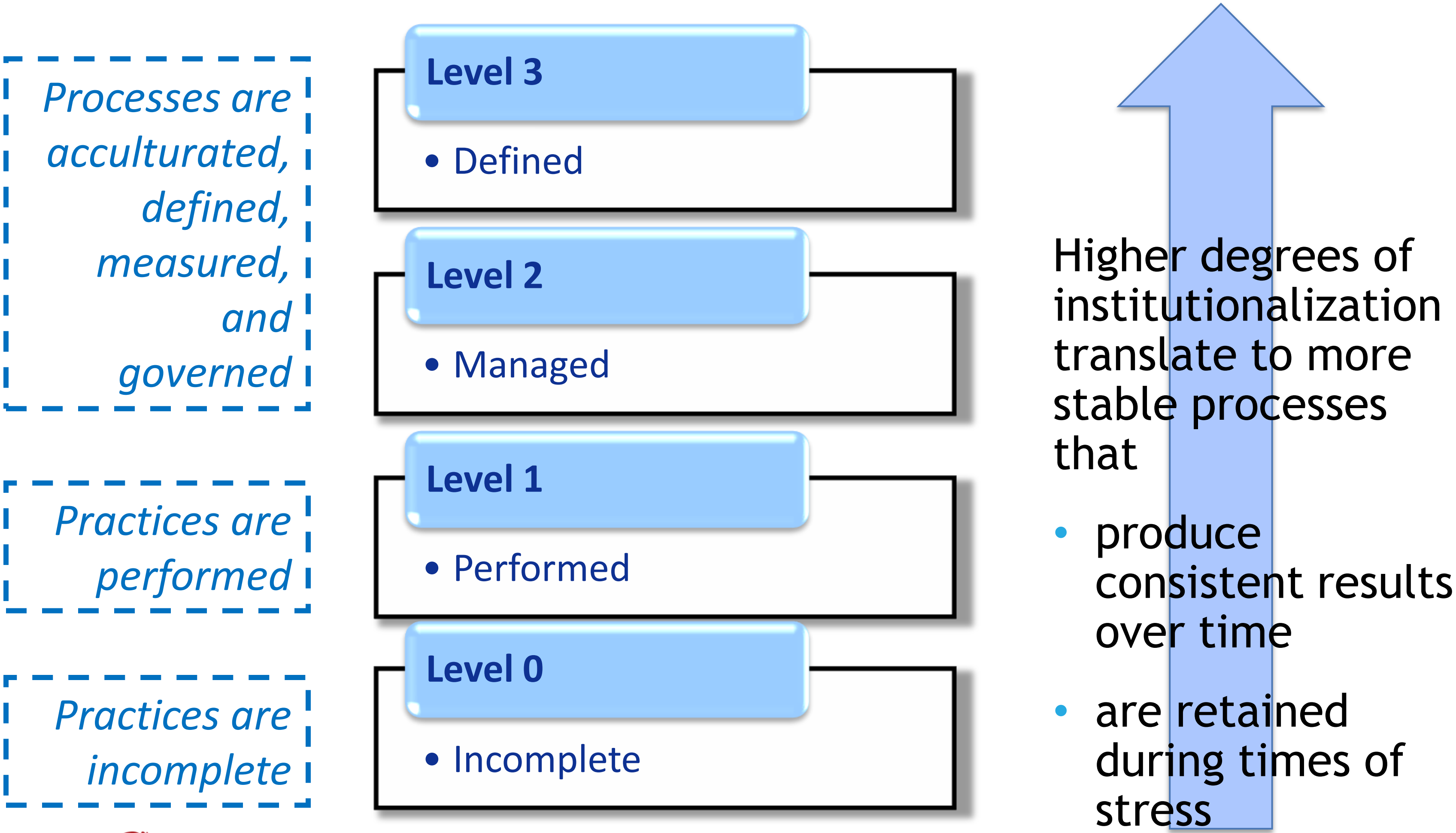
Operations Management

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

Process Management

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

Process Institutionalization in CERT-RMM



Processes are acculturated, defined, measured, and governed

Practices are performed

Practices are incomplete

Level 3

- Defined

Level 2

- Managed

Level 1

- Performed

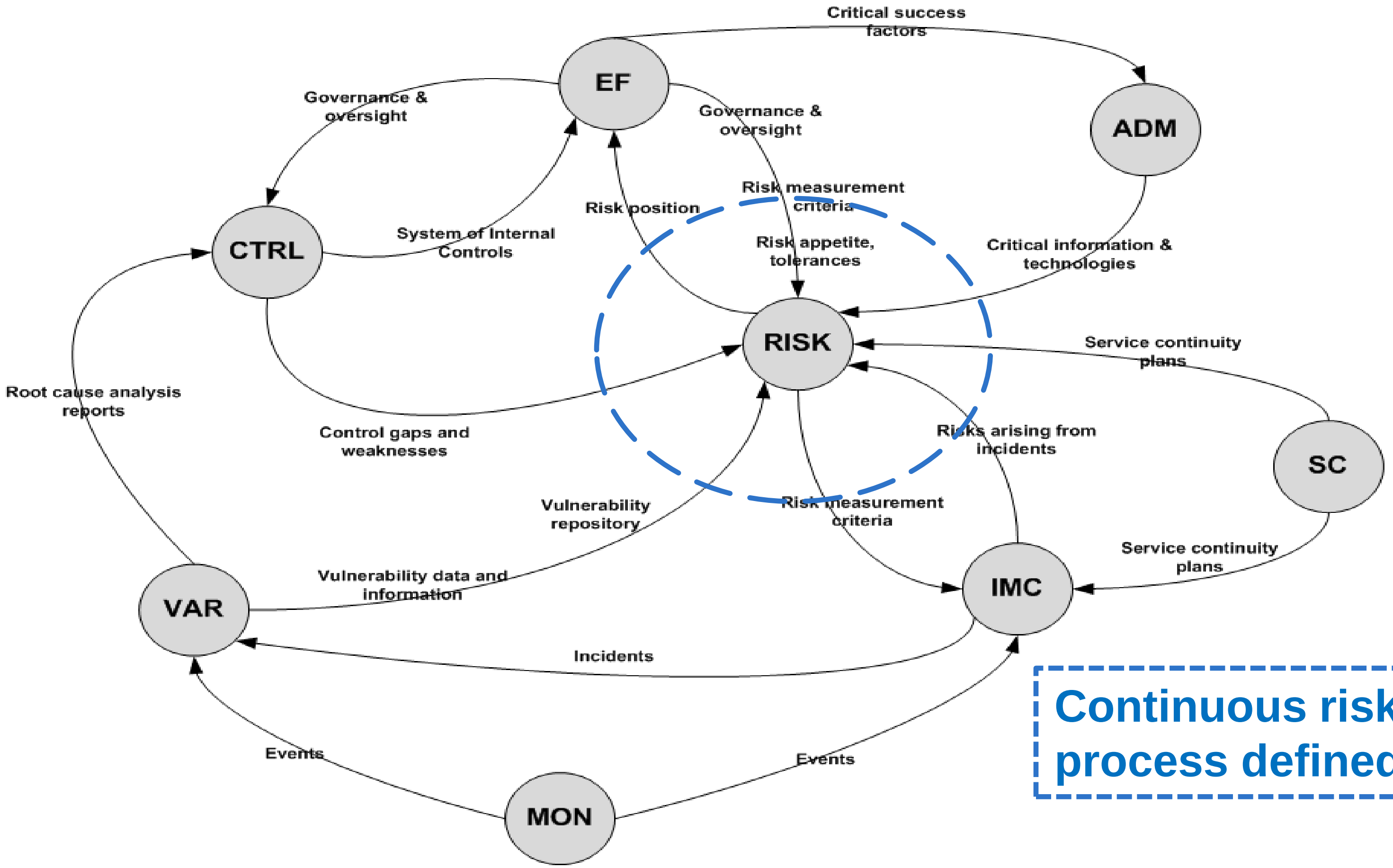
Level 0

- Incomplete

Higher degrees of institutionalization translate to more stable processes that

- produce consistent results over time
- are retained during times of stress

A Risk "Ecosystem" in CERT-RMM


Critical success factors
EF
Governance & oversight
Governance & oversight
ADM
System of Internal Controls
Risk position
Risk measurement criteria
CTRL
Risk appetite, tolerances
Critical information & technologies
RISK
Service continuity plans
Root cause analysis reports
Control gaps and weaknesses
Risks arising from incidents
SC
Vulnerability repository
Risk measurement criteria
Service continuity plans
Vulnerability data and information
IMC
VAR
Incidents
Events
Events
MON

Continuous risk management process defined and executed

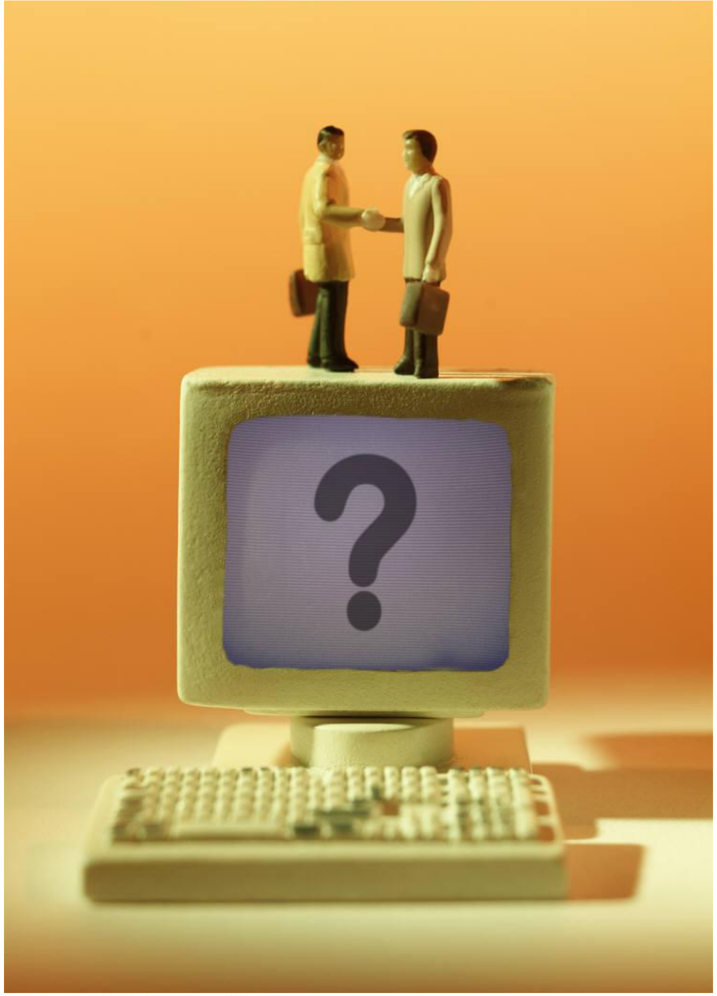
Summary

- We’ve given you a common, structured way to discuss
  - Elements of Risk
    - Condition
    - Consequence
    - Uncertainty
  - Operational Risks
  - Continuous Risk Management
  - Vulnerability Assessment
  - Resilience
- We’ve also introduced CERT-RMM, which can help you
  - Improve processes
  - Bring together IT Ops, Security, and BC/DR

Apply - Things To Do Next Week

- Start a conversation (IT, Security, and BC/DR *should* all be working together)
- Try to answer any two of our opening "questions to consider" in your organization.
- Choose one RMM process area and start working through the specific practices.

Questions?



www.cert.org/resilience

Julia Allen
RMM Developer/Measurement Team Lead
jha@sei.cmu.edu

David White
RMM Transition Lead & Developer
dwhite@cert.org

Rich Caralli
Technical Manager,
Resilient Enterprise Management
rcaralli@cert.org

Joe McLeod
For info on working with us
jmcleod@sei.cmu.edu

Jim Cebula
Information Resilience Team Lead
jcebula@cert.org

Lisa Young
RMM Appraisal Lead & Developer
lry@cert.org

SEI Customer Relations
customer-relations@sei.cmu.edu

412-268-5800

Richard Lynch
Public Relations — All Media Inquiries
public-relations@sei.cmu.edu

NO WARRANTY

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE 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.

Use of any trademarks in this presentation is not intended in any way to infringe on the rights of the trademark holder.