# Overview of the CERT® Resilience Management Model (CERT®-RMM)

Jim Cebula
Technical Manager - Cyber Risk Management, CERT® Division

Jim Cebula is the Technical Manager of the Cyber Risk Management team in the Cyber Security Solutions Directorate of the CERT Division at the Software Engineering Institute (SEI), a unit of Carnegie Mellon University.

Cebula's current activities include risk management methods along with assessment and management of operational resilience among Federal departments and agencies as well as critical infrastructure and key resource (CIKR) providers. He is the co-author of the Taxonomy of Operational Cyber Security Risks, and has instructed courses in the OCTAVE method. He is also currently a co-PI on a research initiative studying perceptions of risk. He joined CERT in 2009 after spending nearly fifteen years in project management, IT and security roles supporting government agencies, most recently as a cyber security manager.

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **23 JAN 2014** | | **00-00-2014 to 00-00-2014** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **Overview of the CERT Resilience Management Model (CERT-RMM)** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon University ,Software Engineering Institute,Pittsburgh,PA,15213** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES

14. ABSTRACT

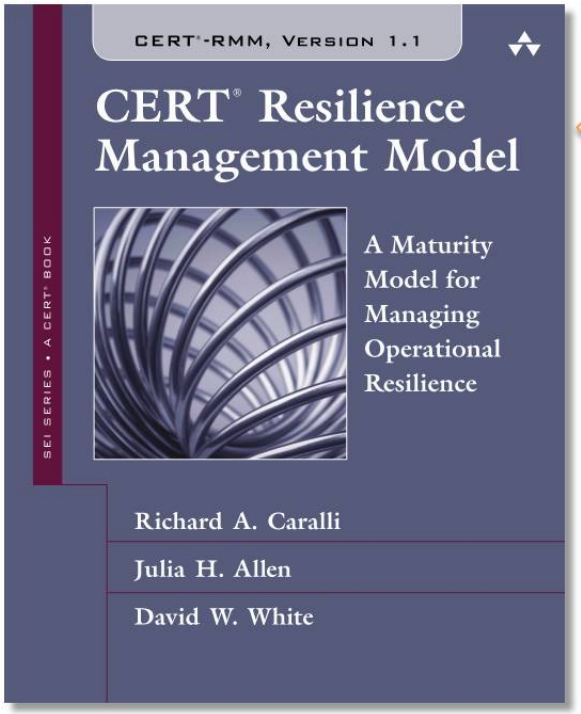
15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT **unclassified** | b. ABSTRACT **unclassified** | c. THIS PAGE **unclassified** | **Same as Report (SAR)** | **55** | |

# Contents

# Background & History

# 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

# What is CERT-RMM?

Guides implementation and management of operational resilience activities

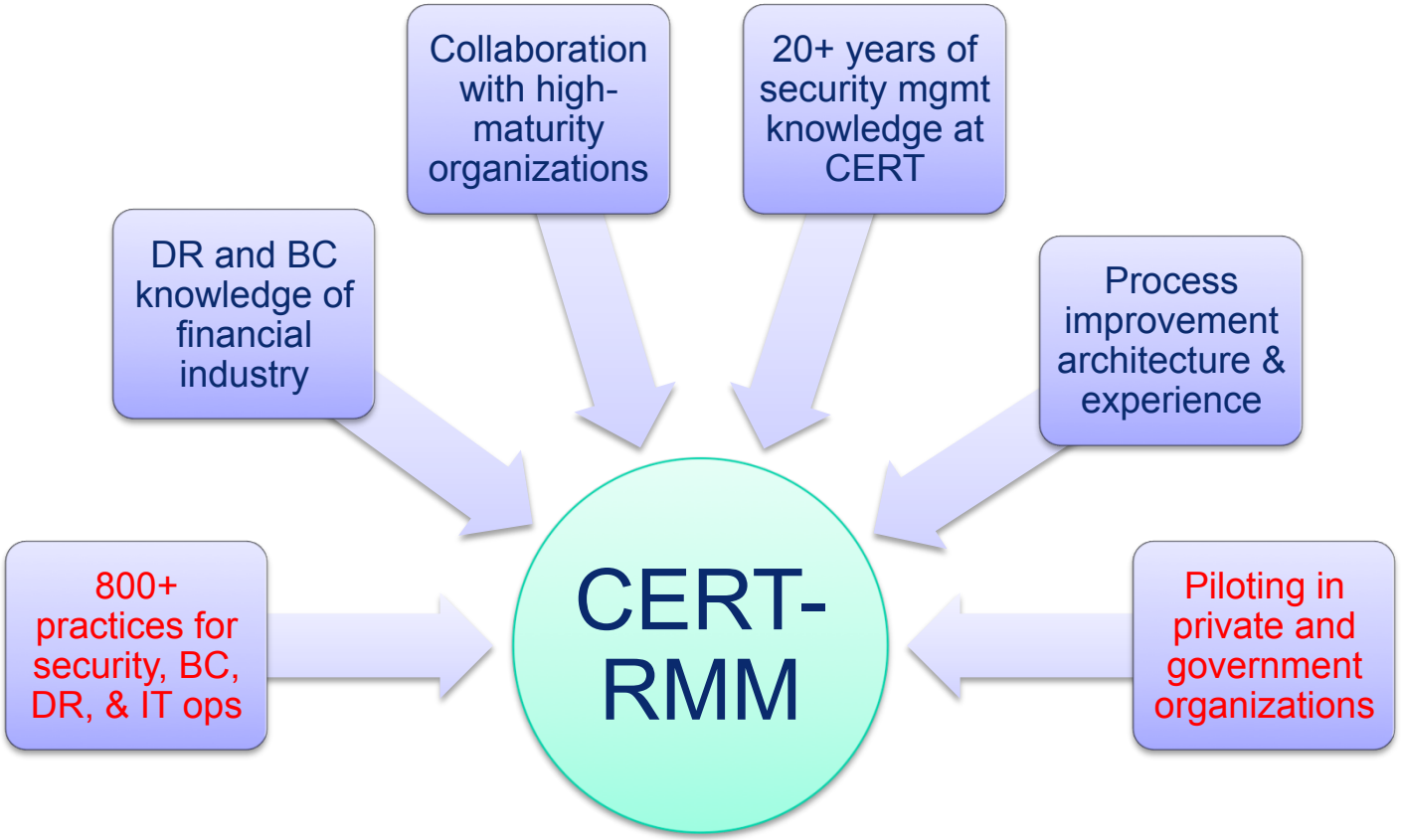
Enables and promotes the **convergence** of

- Business Continuity, COOP, IT disaster recovery
- Information security, cybersecurity
- IT operations

Applicable to a variety of organizations

- small or large
- simple or complex
- public or private

# How was CERT-RMM developed?




CERT-RMM codifies best practices for info. sec., IT DR, and BC from world leading organizations and numerous standards and codes of practice.

# What drove development of CERT-RMM?

Increasingly complex operational environments

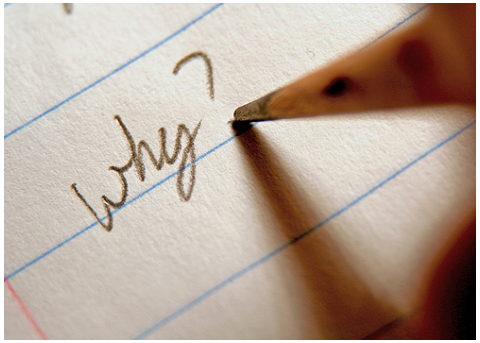
Siloed nature of operational risk activities

Lack of common language or taxonomy

Overreliance on technical approaches

Lack of means to measure organizational capability

Inability to confidently predict outcomes, behaviors, and performance under times of stress



# CERT-RMM – The Model

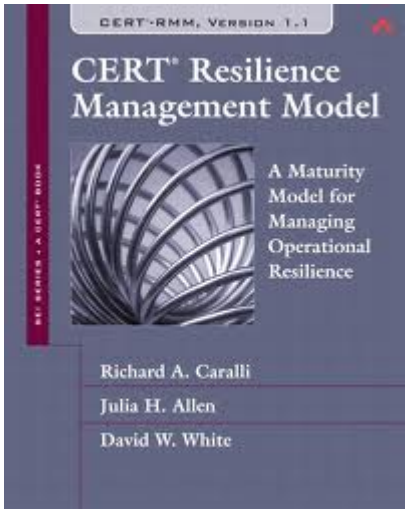
Guidelines and practices for

- converging of security, business continuity, disaster recovery, and IT ops
- implementing, managing, and sustaining operational resilience activities
- managing operational risk through process
- measuring and institutionalizing the resilience process

Common vernacular and basis for planning, communicating, and evaluating improvements

Focuses on “what,” not “how”

Organized into 26 process areas



# CERT-RMM Process Areas

| | |
|---|---|
| Access Management | Measurement and Analysis |
| Asset Definition and Management | Monitoring |
| Communications | Organizational Process Focus |
| Compliance | Organizational Process Definition |
| Controls Management | Organizational Training & Awareness |
| Enterprise Focus | People Management |
| Environmental Control | Resiliency Requirements Development |
| External Dependencies | Resiliency Requirements Management |
| Financial Resource Management | Resilient Technical Solution Engr. |
| Human Resource Management | Risk Management |
| Identity Management | Service Continuity |
| Incident Management & Control | Technology Management |
| Knowledge & Information Mgmt. | Vulnerability Analysis & Resolution |

# Foundational Elements of CERT-RMM

# Foundational Elements of CERT-RMM

Operational Resilience

Risk Management

- Operational Risk Management

Convergence

Organizational Construct for Resilience Activities

Capability Dimension

- Process Institutionalization

Code of Practice Crosswalk

# RISK

1. An event or condition
2. A consequence or impact from the condition
3. An uncertainty

The possibility of suffering a harmful event

Exposure to the chance of injury or loss

The possibility of suffering harm or loss

A source of danger

# RISK Management

- Identify
- Characterize
- Assess
- Prioritize
- Mitigate
- Avoid
- Reduce
- Accept
- Share
- Monitor
- Etc…

# Operational Risk Management

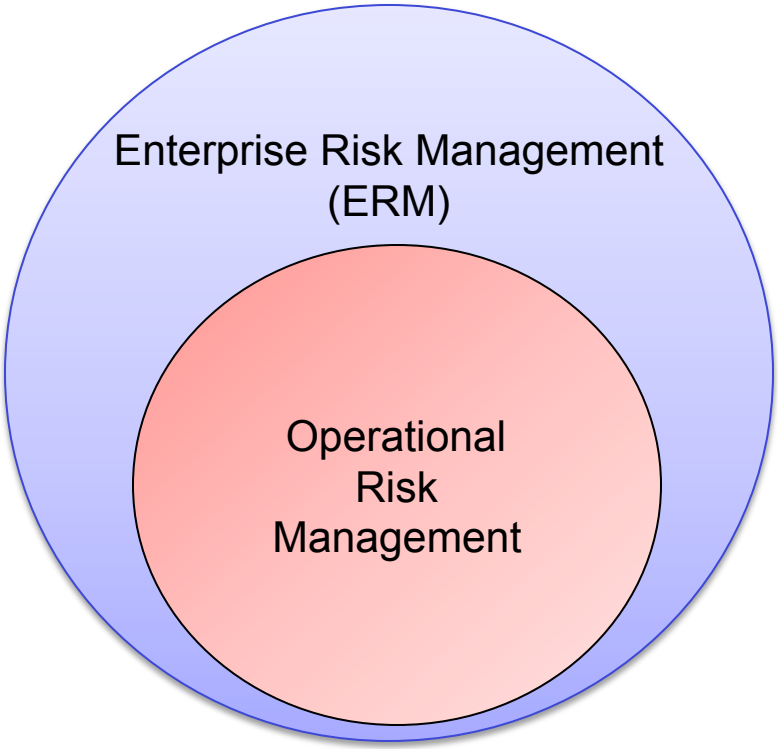
A form of risk affecting day-to-day business operations

A very broad risk category

- from high-frequency, low-impact to low-frequency, high-impact

Types of Operational Risks

- actions of people
- systems and technology failures
- failed internal processes
- external events




Operational resilience emerges from effective management of operational risk.

# Hurdles to Effective Operational Risk & Resilience Mgmt.

Vague and abstract nature

Compartmentalization

Technology focus

Practice proliferation

Insufficient funding

Insufficient success metrics

Discrete nature of activity

(Over)reliance on people

Regulatory climate

Head-in-the-sand

# Cornerstones & Foundational Elements of CERT-RMM

- ✓ Operational Resilience
- ✓ Operational Risk Management
- Convergence
- Organizational Construct for Resilience Activities

- Protection and Sustainment Activities
- Institutionalization
- Lifecycle View
- Code of Practice Crosswalk

# Convergence

A fundamental concept in managing operational resilience

Refers to the harmonization of operational risk management activities that have similar objectives and outcomes

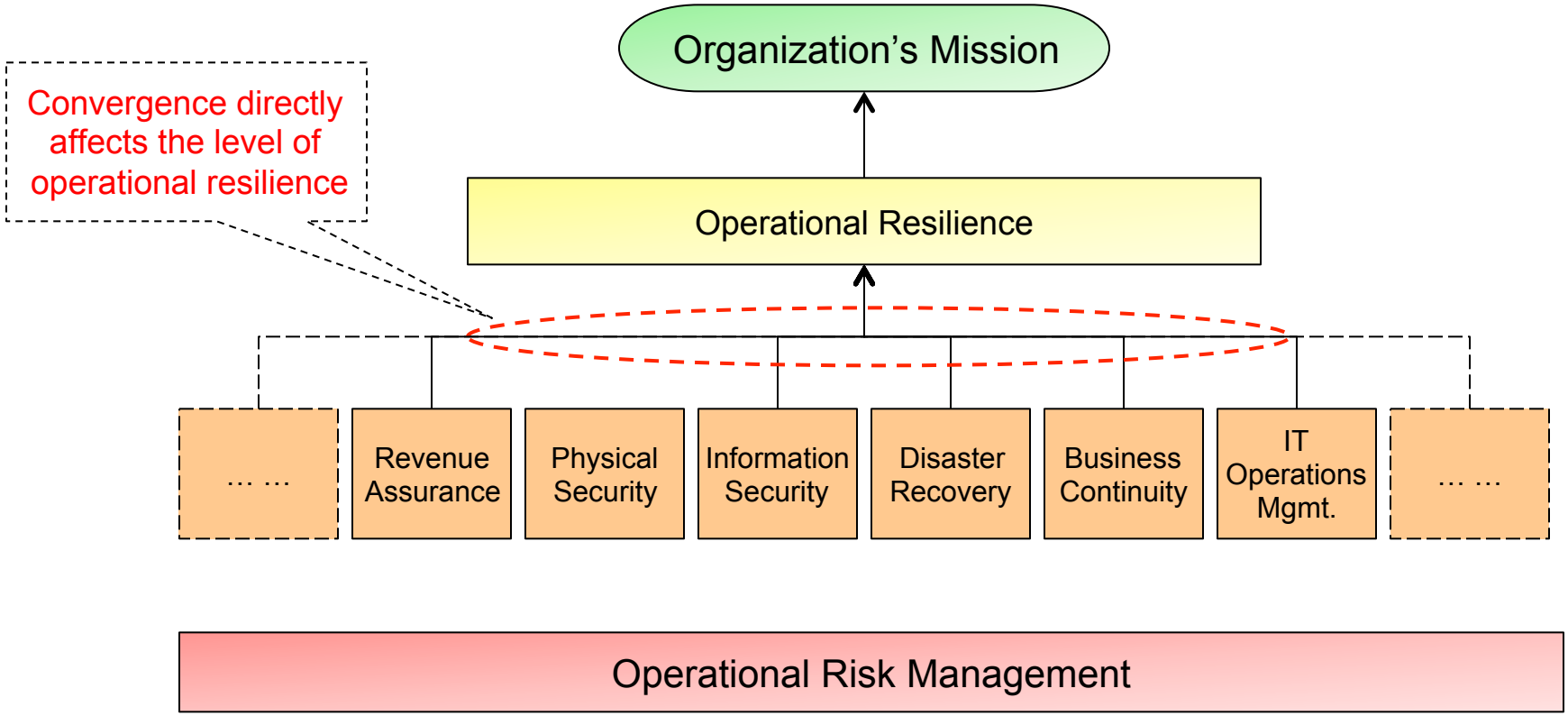
Operational risk management activities include (but are not limited to)

- security planning and management
- business continuity and disaster recovery
- IT operations and service delivery management

Other support activities may also be involved

- communications
- financial management
- etc.

# Convergence



# Benefits of Convergence and Integration

Similar activities are bound by the same risk drivers

Allows for better alignment between risk-based activities and organizational risk tolerances and appetite

Eliminates redundant activities (and associated costs)

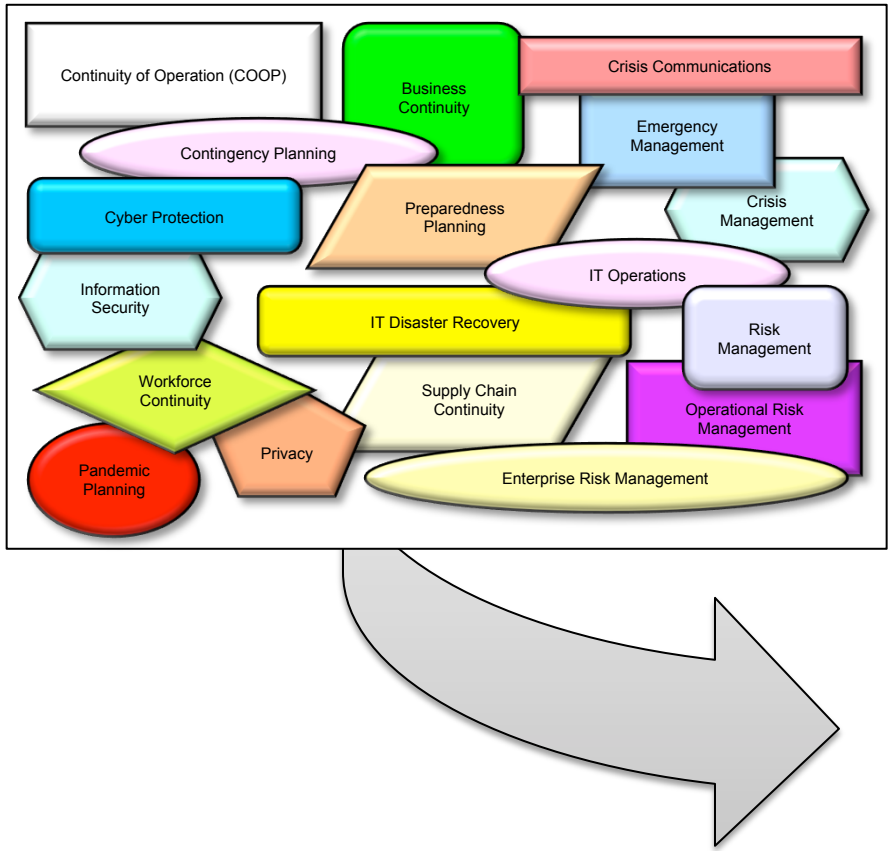
Forces collaboration between activities that have similar objectives

Enforces a mission focus

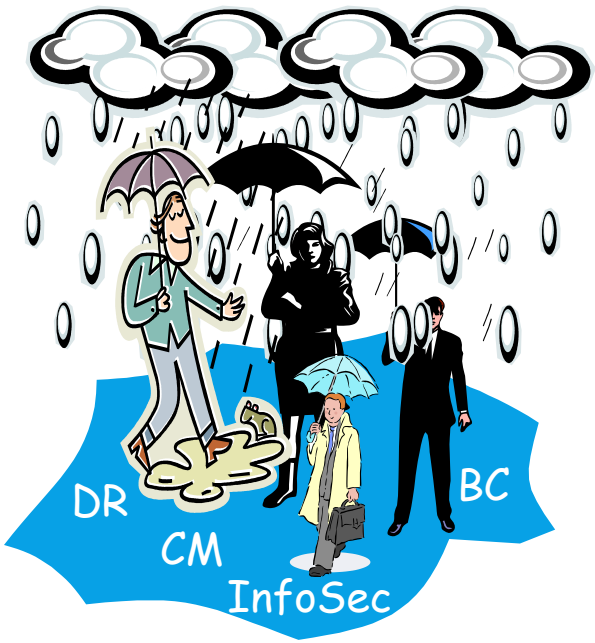
Facilitates a process that is owned across the organization

Influences how operational risk and resilience management work is planned, executed, and managed

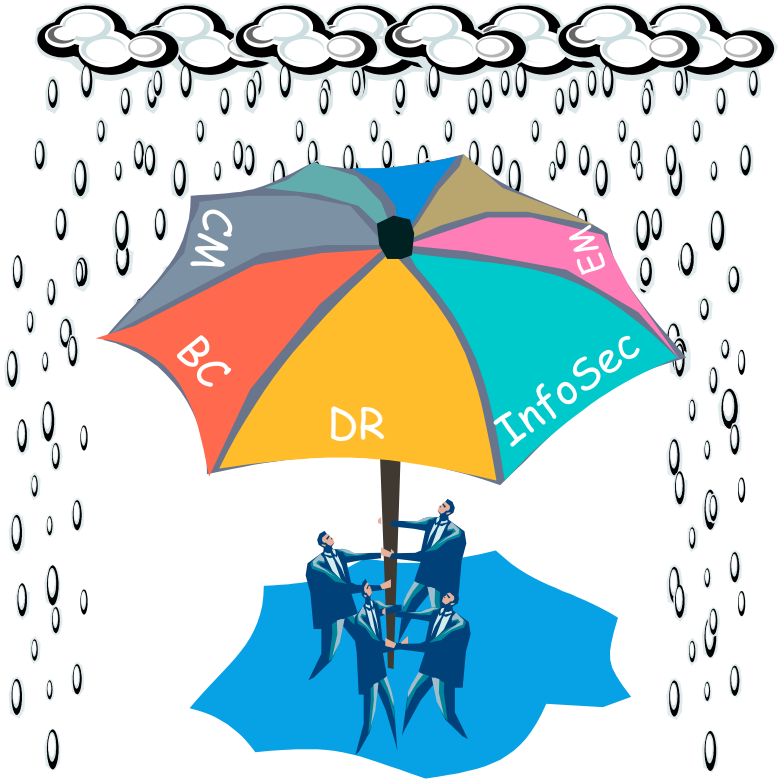
# Desired Integrated Approach




# Desired Integrated Approach




Convergence



# Enemies of Convergence

Organizational structures

Traditional funding models

Overuse and misuse of codes of practice

Unclear or poorly defined and communicated risk drivers

Unclear or poorly defined enterprise objectives, strategic objectives, and critical success factors

Lack of supporting process orientation and definition

Lack of sponsorship and governance for the process

Lack of a risk-aware culture

# Cornerstones & Foundational Elements of CERT-RMM

- ✓ Operational Resilience
- ✓ Operational Risk Management
- ✓ Convergence

Organizational Construct for Resilience Activities

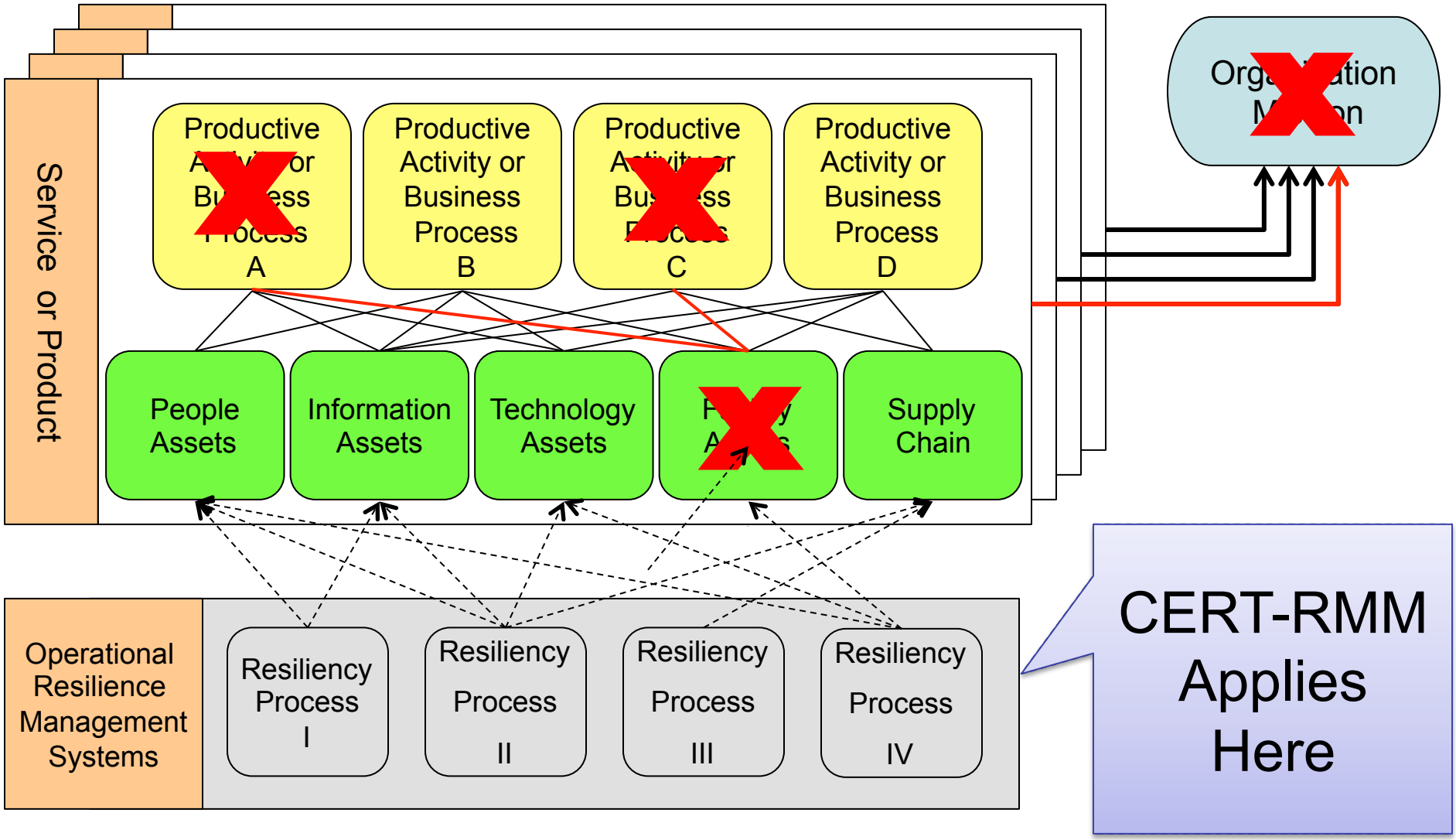
Protection and Sustainment Activities

Institutionalization

Lifecycle View

Code of Practice Crosswalk

# Organizational Context for Resilience Activities



# Cornerstones & Foundational Elements of CERT-RMM

- Operational Resilience
- Operational Risk Management
- Convergence
- Organizational Construct for Resilience Activities

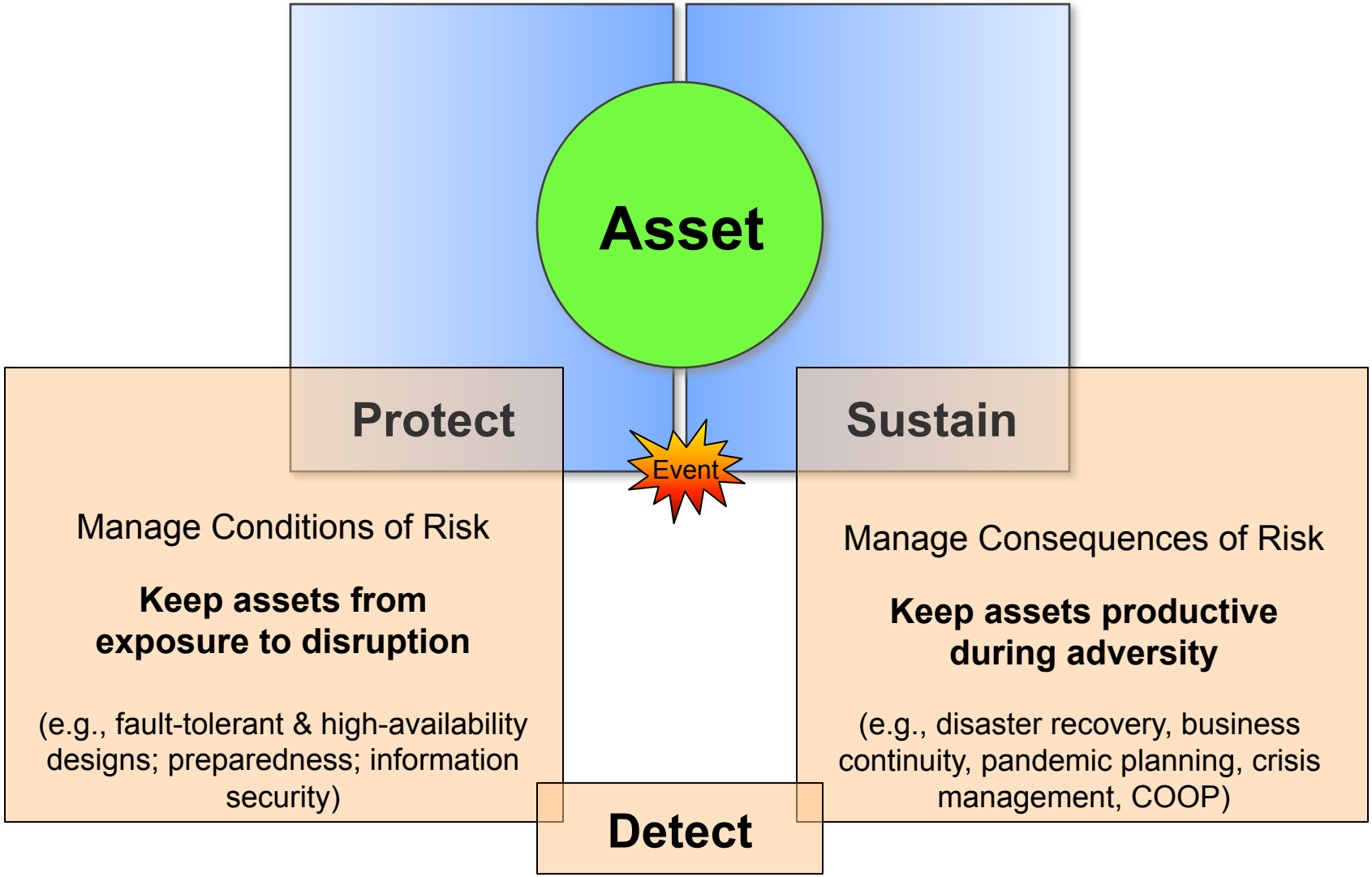
Protection and Sustainment Activities

Institutionalization

Lifecycle View

Code of Practice Crosswalk

# Operational Resilience Starts at the Asset Level



# Cornerstones & Foundational Elements of CERT-RMM

- Operational Resilience
- Operational Risk Management
- Convergence
- Organizational Construct for Resilience Activities

- Protection and Sustainment Activities

Institutionalization

Lifecycle View

Code of Practice Crosswalk

# What do these organizations have in common?

Customer Happiness

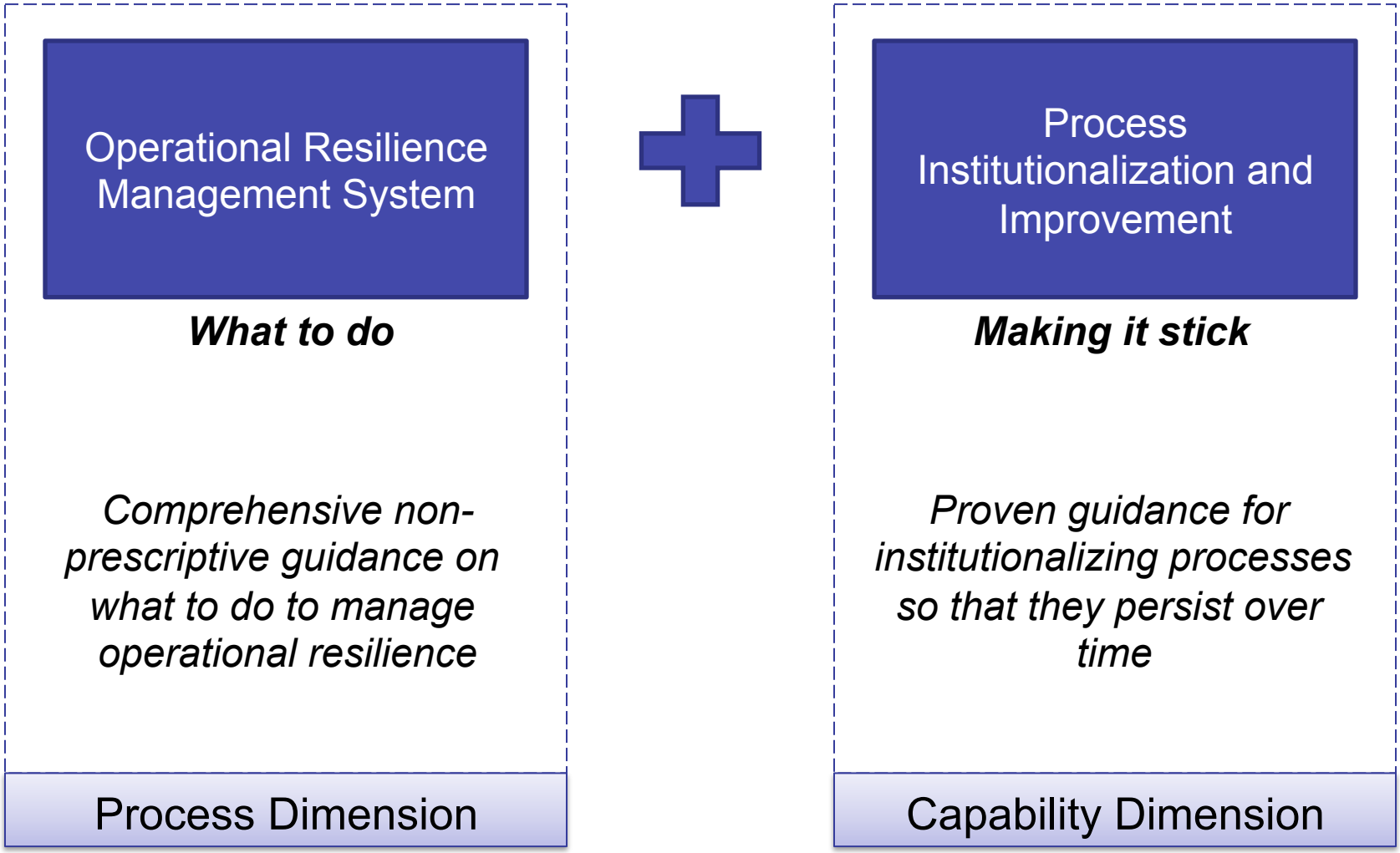

Chain of Command
Unit Cohesion
Regulations


Strong Culture


Customer Service

Tradition
Protection

# CERT-RMM Combines Two Approaches



# Institutionalizing a Culture of Resilience

**institutionalize** *verb* (CUSTOM) (UK USUALLY **institutionalise**) UK US /ɪnt.stɪ'tjuː.ʃᵊn.ə.laɪz/ US /-'tuː-/ [T]

to make something become part of a particular society, system, or organization

*What was once an informal event has now become institutionalized.*

Organizations must provide explicit guidance for institutionalizing resilience activities so that they persist over time.

Ask not "how well am I performing today?"

Ask "do I have what it takes to sustain high performance beyond today?"

# Cornerstones & Foundational Elements of CERT-RMM

- Operational Resilience
- Operational Risk Management
- Convergence
- Organizational Construct for Resilience Activities

- Protection and Sustainment Activities
- Institutionalization

Lifecycle View

Code of Practice Crosswalk

# Lifecycle View


Resilience Engineering

Protection and Sustainment Activities

To improve and sustain an entity's operational resilience, it is not sufficient to improve only protection and sustainment activities.

Resilience should not be an afterthought bolt-on.

Resilience should be engineered and built in.

Resilience Management is a Total Lifecycle Concept.

# Cornerstones & Foundational Elements of CERT-RMM

- Operational Resilience
- Operational Risk Management
- Convergence
- Organizational Construct for Resilience Activities

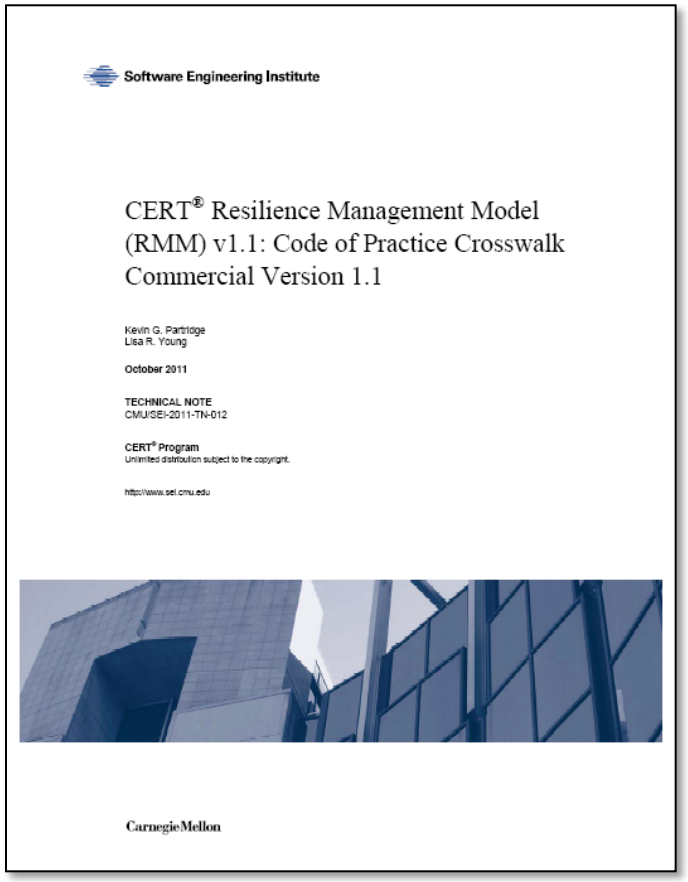
- Protection and Sustainment Activities
- Institutionalization
- Lifecycle View

Code of Practice Crosswalk

# Code of Practice Crosswalk

Links CERT-RMM practices to commonly used codes of practice and standards, including

- ANSI/ASIS SPC.1-2009
- BS25999
- COBIT 4.1
- COSO ERM Framework
- CMMI
- FFIEC BCP Handbook
- ISO 20000-2
- ISO/IEC 24762
- ISO/IEC 24762
- ISO/IEC 27005
- ISO/IEC 31000
- NFPA 1600
- PCI DSS
- etc.



# CERT-RMM Code of Practice Crosswalk

| Process Area Specific Goals and Specific Practices | ANSI/ASIS SPC.1-2009 | BS25999-1: 2006 | CMMI-Dev | CMMI-Svc | COBIT 4.1 | FFIEC BCP Handbook | ISO/IEC 20000-2: 2005 (E) | ISO/IEC 24762: 2008 (E) | ISO/IEC 27002: 2005 (E) | ISO/IEC 27005: 2008 (E) | ISO/IEC 31000: 2009 (E) | NFPA 1600 | PCI: 2009 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| SC:SG5.SP4 Evaluate Plan Test Results<br>Subpractices<br>1. Compare actual test results with expected test results and test objectives.<br>2. Document areas of improvement for service continuity plans.<br>3. Document areas of improvement for testing service continuity plans | 4.5.3 | 5.4.1<br>9.3.2 | | SCON:SP3.3 | DS4.5 | Board and Senior Manage-ment Re-sponsibility<br>Risk As-sessment<br>Risk Man-agement<br>Risk Moni-toring and Testing<br>Appendix H: Testing Program- | 6.3.4 | 5.10<br>6.15.4 | 14.1.5 | | | 7.5 | |

Extensive Tabular Crosswalk between CERT-RMM's 26 process areas and 251 specific practices and key industry standards

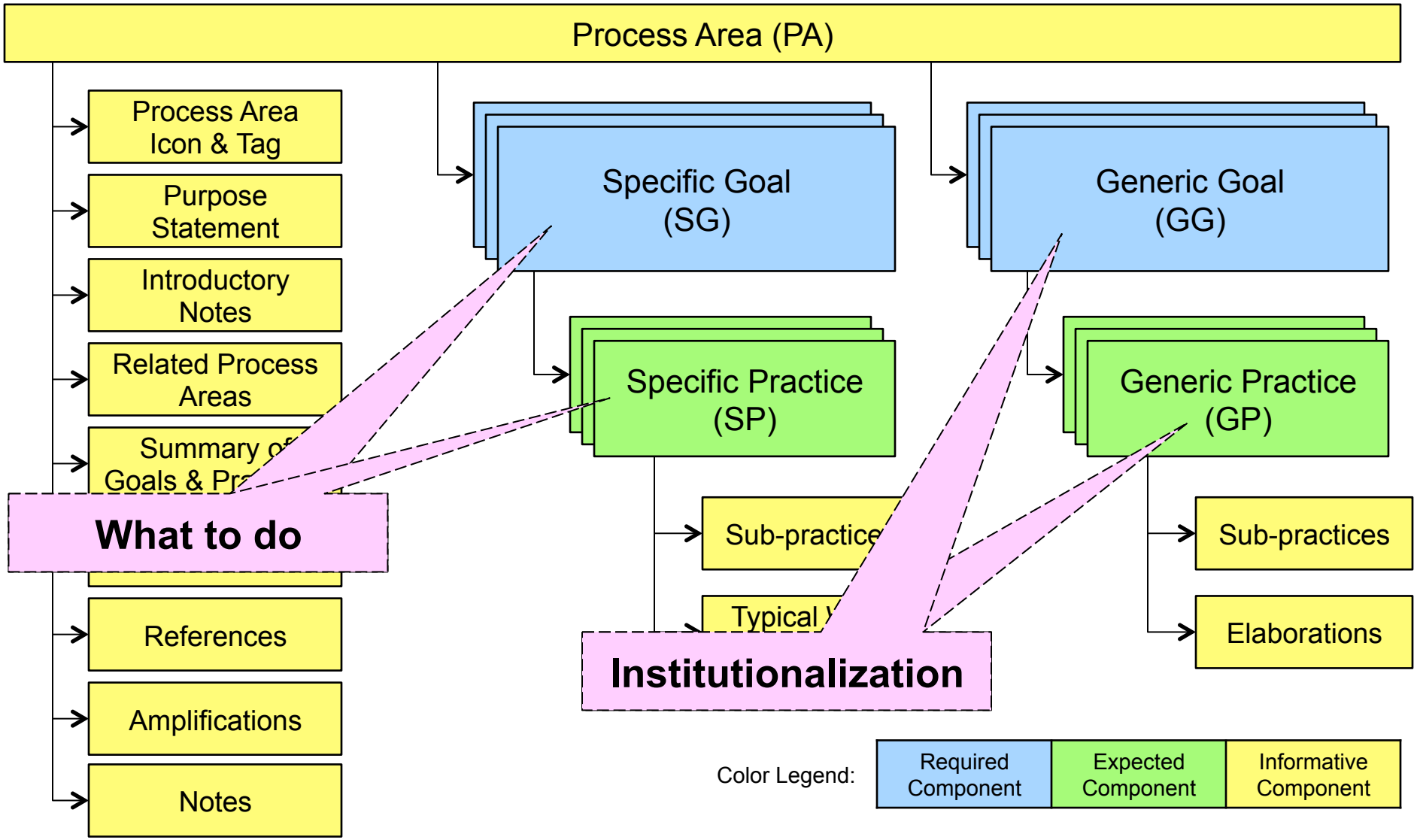
# Cornerstones & Foundational Elements of CERT-RMM

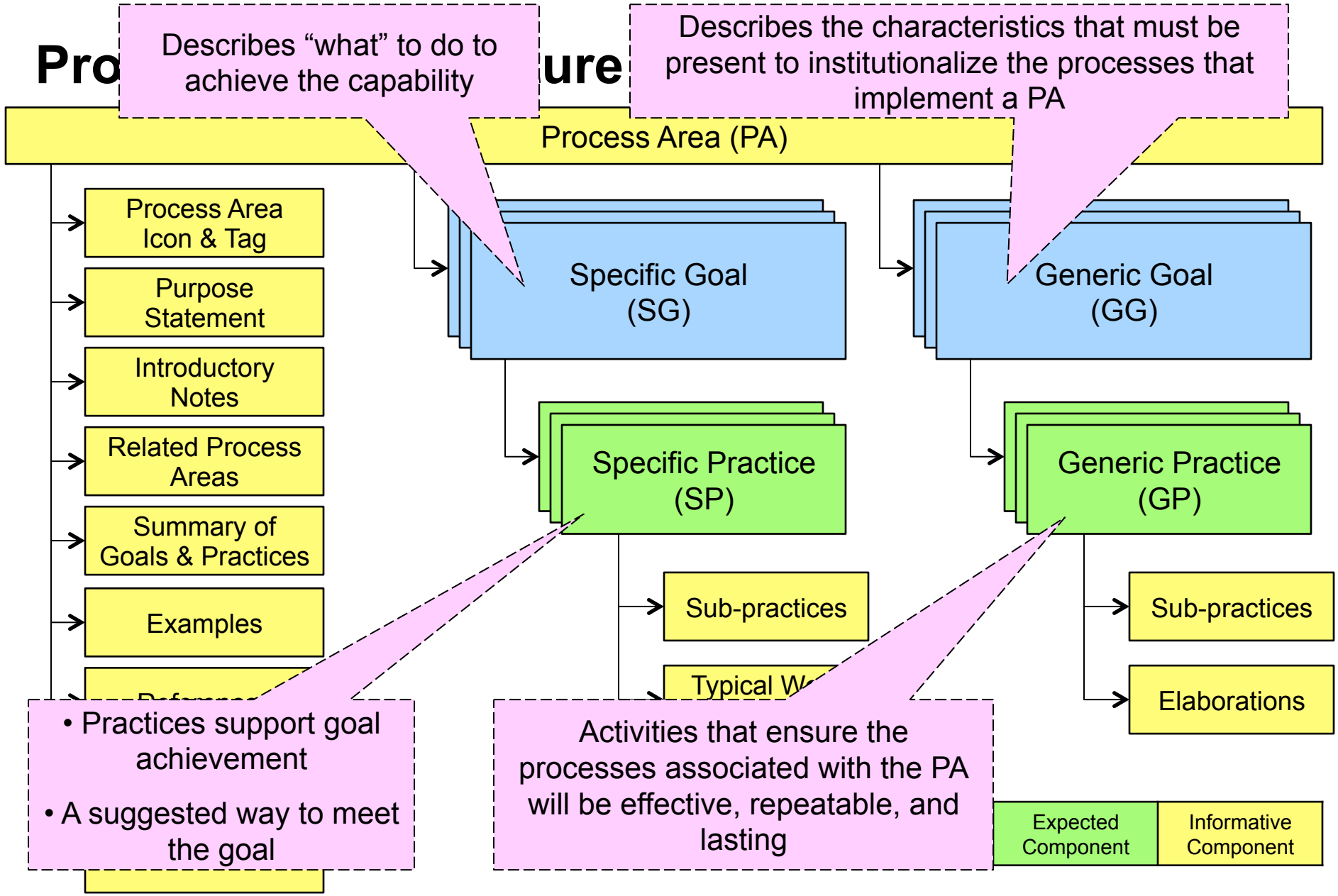
- Operational Resilience
- Operational Risk Management
- Convergence
- Organizational Construct for Resilience Activities

- Protection and Sustainment Activities
- Institutionalization
- Lifecycle View
- Code of Practice Crosswalk

# Organization of the Model

# Process Area Structure & Components





# Example: Service Continuity Process Area

| | |
|---|---|
| Access Management | Measurement and Analysis |
| Asset Definition and Management | Monitoring |
| Communications | Organizational Process Focus |
| Compliance | Organizational Process Definition |
| Controls Management | Organizational Training & Awareness |
| Enterprise Focus | People Management |
| Environmental Control | Resiliency Requirements Development |
| External Dependencies | Resiliency Requirements Management |
| Financial Resource Management | Resilient Technical Solution Engr. |
| Human Resource Management | Risk Management |
| Identity Management | **Service Continuity** |
| Incident Management & Control | Technology Management |
| Knowledge & Information Mgmt | Vulnerability Analysis & Resolution |

# Example: Service Continuity Process Area

## SERVICE CONTINUITY


### Purpose

The purpose of Service Continuity is to ensure the continuity of essential operations of services and related assets if a disruption occurs as a result of an incident, disaster, or other disruptive event.

### Introductory Notes

The continuity of an organization's service delivery is a paramount concern in the organization's operational resilience activities. The organization can invest considerable time and resources in attempting to prevent a range of potential disruptive events, but no organization can mitigate all risk. As a result, the organization must be prepared to deal with the consequences of a disruption to its operations at any time. Significant disruption can result in dire circumstances for the organization, even bankruptcy or termination.

# Example: Service Continuity Process Area

## Summary of Specific Goals and Practices

SC:SG1 Prepare for Service Continuity

- SC:SG1.SP1 Plan for Service Continuity
- SC:SG1.SP2 Establish Standards and Guidelines for Service Continuity

SC:SG2 Identify and Prioritize High-Value Services

- SC:SG2.SP1 Identify the Organization's High-Value Services
- SC:SG2.SP2 Identify Internal and External Dependencies and Interdependencies
- SC:SG2.SP3 Identify Vital Organizational Records and Databases

SC:SG3 Develop Service Continuity Plans

- SC:SG3.SP1 Identify Plans to Be Developed
- SC:SG3.SP2 Develop and Document Service Continuity Plans
- SC:SG3.SP3 Assign Staff to Service Continuity Plans
- SC:SG3.SP4 Store and Secure Service Continuity Plans
- SC:SG3.SP5 Develop Service Continuity Plan Training

SC:SG4 Validate Service Continuity Plans

- SC:SG4.SP1 Validate Plans to Requirements and Standards
- SC:SG4.SP2 Identify and Resolve Plan Conflicts

# Example: Service Continuity Process Area

**SC:SG2.SP1** *IDENTIFY THE ORGANIZATION'S HIGH-VALUE SERVICES*

*The high-value services of the organization and their associated assets are identified.*

*The identification and prioritization of the organization's high-value services as strategic planning activities are addressed in the Enterprise Focus process area. This practice is included here to emphasize the importance of prioritizing high-value services as a founda-*

*Typical work products*

1. Prioritized list of high-value organizational services, activities, and associated assets
2. Results of security risk assessment and business impact analyses

*Subpractices*

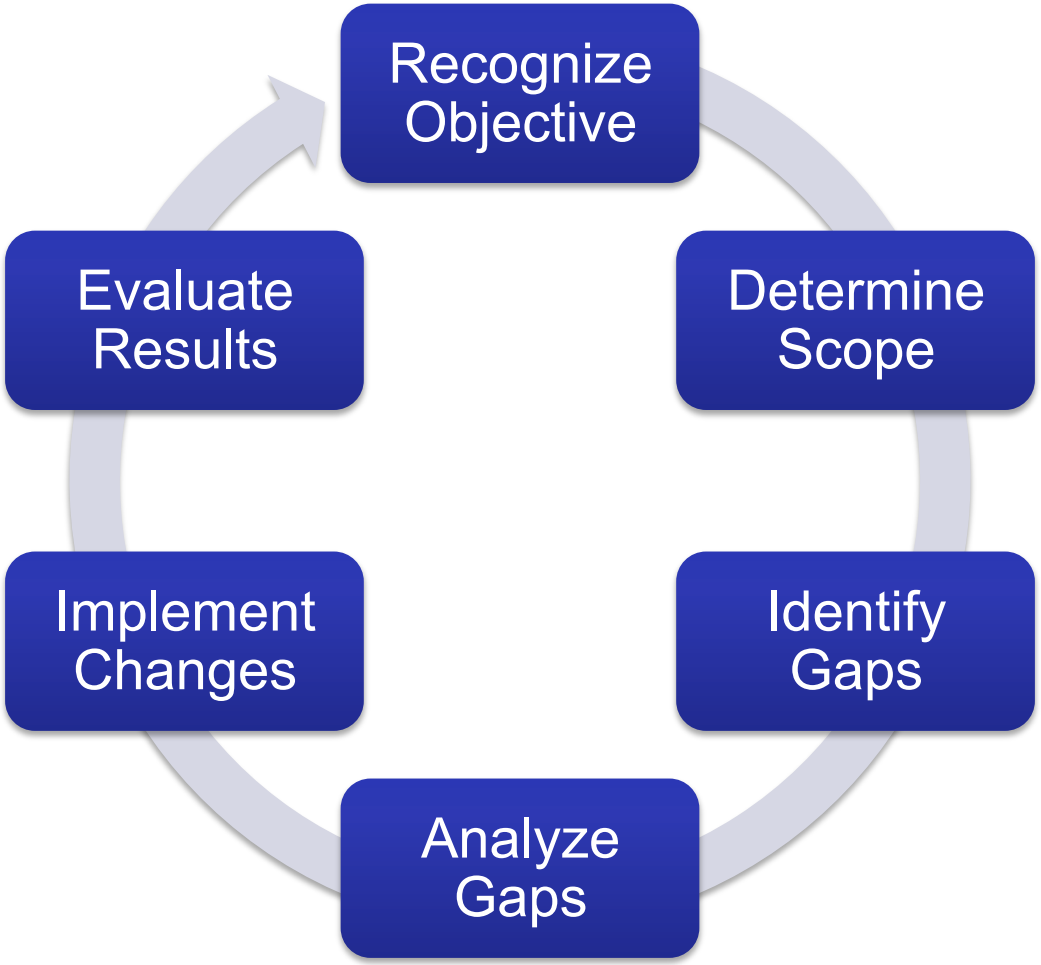
1. Identify the organization's high-value services, associated assets, and activities.
2. Analyze and document the relative value of providing these services and the resulting impact on the organization if these services are interrupted.

   Consideration of the consequences of the loss of high-value organizational services is typically performed as part of a business impact analysis. In addition, the conse-

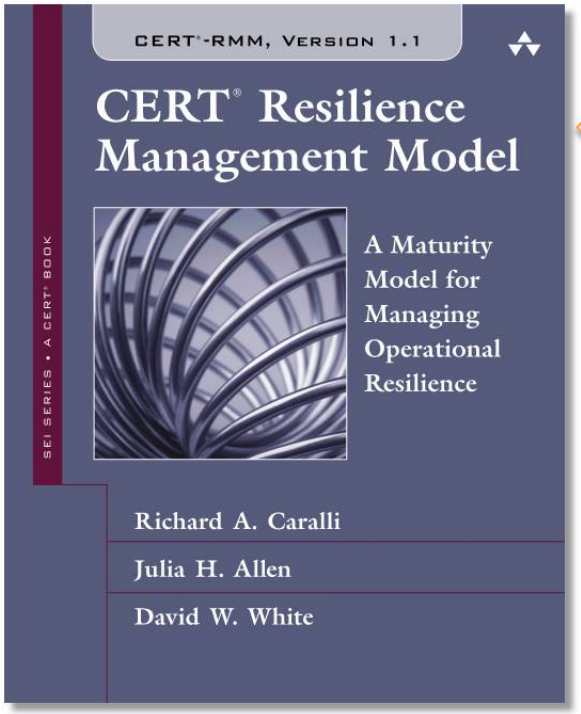
   quences of risks to high-value services are identified and analyzed in risk assess-

# Using the Model

# Using CERT-RMM for improvement



# 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

# For FISMA Compliance

| |
|---|
| Access Management |
| Asset Definition and Management |
| Communications |
| Compliance |
| Controls Management |
| Enterprise Focus |
| Environmental Control |
| External Dependencies |
| Financial Resource Management |
| Human Resource Management |
| Identity Management |
| Incident Management & Control |
| Knowledge & Information Mgmt |

| |
|---|
| Measurement and Analysis |
| Monitoring |
| Organizational Process  Focus |
| Organizational Process Definition |
| Organizational Training & Awareness |
| People Management |
| Resiliency Requirements Development |
| Resiliency Requirements Management |
| Resilient Technical Solution Engr. |
| Risk Management |
| Service Continuity |
| Technology Management |
| Vulnerability Analysis & Resolution |

# For Managing Cloud Computing

| |
|---|
| Access Management |
| Asset Definition and Management |
| Communications |
| Compliance |
| Controls Management |
| Enterprise Focus |
| Environmental Control |
| External Dependencies |
| Financial Resource Management |
| Human Resource Management |
| Identity Management |
| Incident Management & Control |
| Knowledge & Information Mgmt |

| |
|---|
| Measurement and Analysis |
| Monitoring |
| Organizational Process  Focus |
| Organizational Process Definition |
| Organizational Training & Awareness |
| People Management |
| Resiliency Requirements Development |
| Resiliency Requirements Management |
| Resilient Technical Solution Engr. |
| Risk Management |
| Service Continuity |
| Technology Management |
| Vulnerability Analysis & Resolution |

# For Managing the Insider Threat Challenge

| |
|---|
| Access Management |
| Asset Definition and Management |
| Communications |
| Compliance |
| Controls Management |
| Enterprise Focus |
| Environmental Control |
| External Dependencies |
| Financial Resource Management |
| Human Resource Management |
| Identity Management |
| Incident Management & Control |
| Knowledge & Information Mgmt |

| |
|---|
| Measurement and Analysis |
| Monitoring |
| Organizational Process Focus |
| Organizational Process Definition |
| Organizational Training & Awareness |
| People Management |
| Resiliency Requirements Development |
| Resiliency Requirements Management |
| Resilient Technical Solution Engr. |
| Risk Management |
| Service Continuity |
| Technology Management |
| Vulnerability Analysis & Resolution |

# For Managing Disaster Recovery, COOP, and Business Continuity Policies

| |
|---|
| Access Management |
| Asset Definition and Management |
| Communications |
| Compliance |
| Controls Management |
| Enterprise Focus |
| Environmental Control |
| External Dependencies |
| Financial Resource Management |
| Human Resource Management |
| Identity Management |
| Incident Management & Control |
| Knowledge & Information Mgmt |

| |
|---|
| Measurement and Analysis |
| Monitoring |
| Organizational Process  Focus |
| Organizational Process Definition |
| Organizational Training & Awareness |
| People Management |
| Resiliency Requirements Development |
| Resiliency Requirements Management |
| Resilient Technical Solution Engr. |
| Risk Management |
| Service Continuity |
| Technology Management |
| Vulnerability Analysis & Resolution |

# Summary

# Distinguishing Features of CERT-RMM

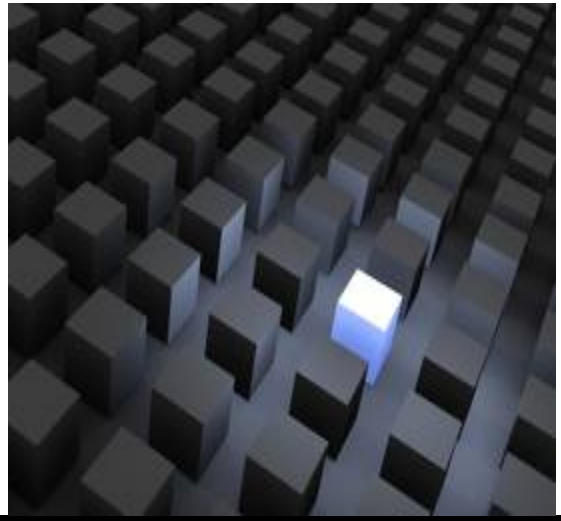
**Converges** key operational risk management activities: security, BC/DR, and IT operations

Guides **implementation and management** of operational resilience activities

**Descriptive** rather than prescriptive: focuses on the "what," not the "how"

Provides an organizing convention for effective selection and deployment of codes of practice and standards

Guides improvement in areas where an organization's capability does not equal its desired state



# Distinguishing Features of CERT-RMM (Cont.)

Improves confidence in how an organization responds in times of operational stress

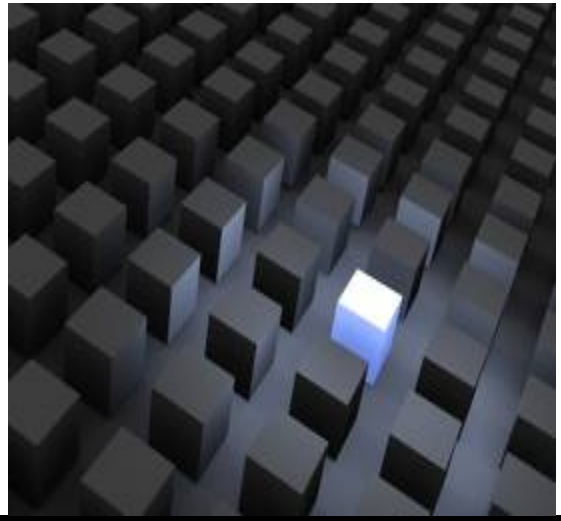
Provides a baseline from which to perform an appraisal

Enables **measurements** of effectiveness

Is a process improvement model

Enables **institutionalization**

Is **not a proprietary** model



# Variety of Ways to Use CERT-RMM

Starting point for **socializing** important harmonization and **convergence** principles across security, business continuity, and IT operations activities

Reference model for understanding the scope of managing operational resilience

Process improvement model to catalyze a process improvement effort

**Baseline** from which to perform an appraisal of an organization's capability

**Guide for improvement** in areas where an organization's capability does not equal its desired state

**Organizing construct for codes of practice**

Taxonomy

# Notices



This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.



DM-0000904


SEI Training

# *Introduction to the CERT Resilience Management Model*

February 18 - 20, 2014 (SEI, Arlington, VA)

June 17 - 19, 2014 (SEI, Pittsburgh, PA)

See Materials Widget for course document