CERT® Resiliency Management Model

Improving and Sustaining Processes for Managing Operational Resiliency

Presentation for New York SPIN

February 9, 2010

David White

RMM Product Manager & Developer

Getting acquainted

By show of hand:

- I am familiar with CMMI
- I am a CMMI Instructor or SCAMPI Lead Appraiser
- I do not know very much about CMMI
- My organization (or my customer) seeks to improve security, IT operations, or business continuity capabilities
- I am familiar with the SEI
- I am familiar with CERT
- I am familiar with RMM

Software Engineering Institute

Federally Funded Research and Development Center (FFRDC) operated by Carnegie Mellon University, established in 1984

Basic and applied research — helping organizations to continually improve the development, operation, and management of software-intensive and networked systems

Widely-known “brands”

- CERT
- Capability Maturity Model Integration (CMMI)

What is RMM?

The CERT® Resiliency Management Model (RMM) is a process improvement model for managing operational resiliency. It promotes the convergence of security, business continuity, and IT operations activities as a means to actively direct, control, and manage operational resiliency and risk.

Agenda

Introduction

Organizational challenges

Building blocks for a resiliency approach

Using CERT-RMM

CERT-RMM activities

Questions?

Organizational challenges

Operating under risk and uncertainty

Setting the operational landscape

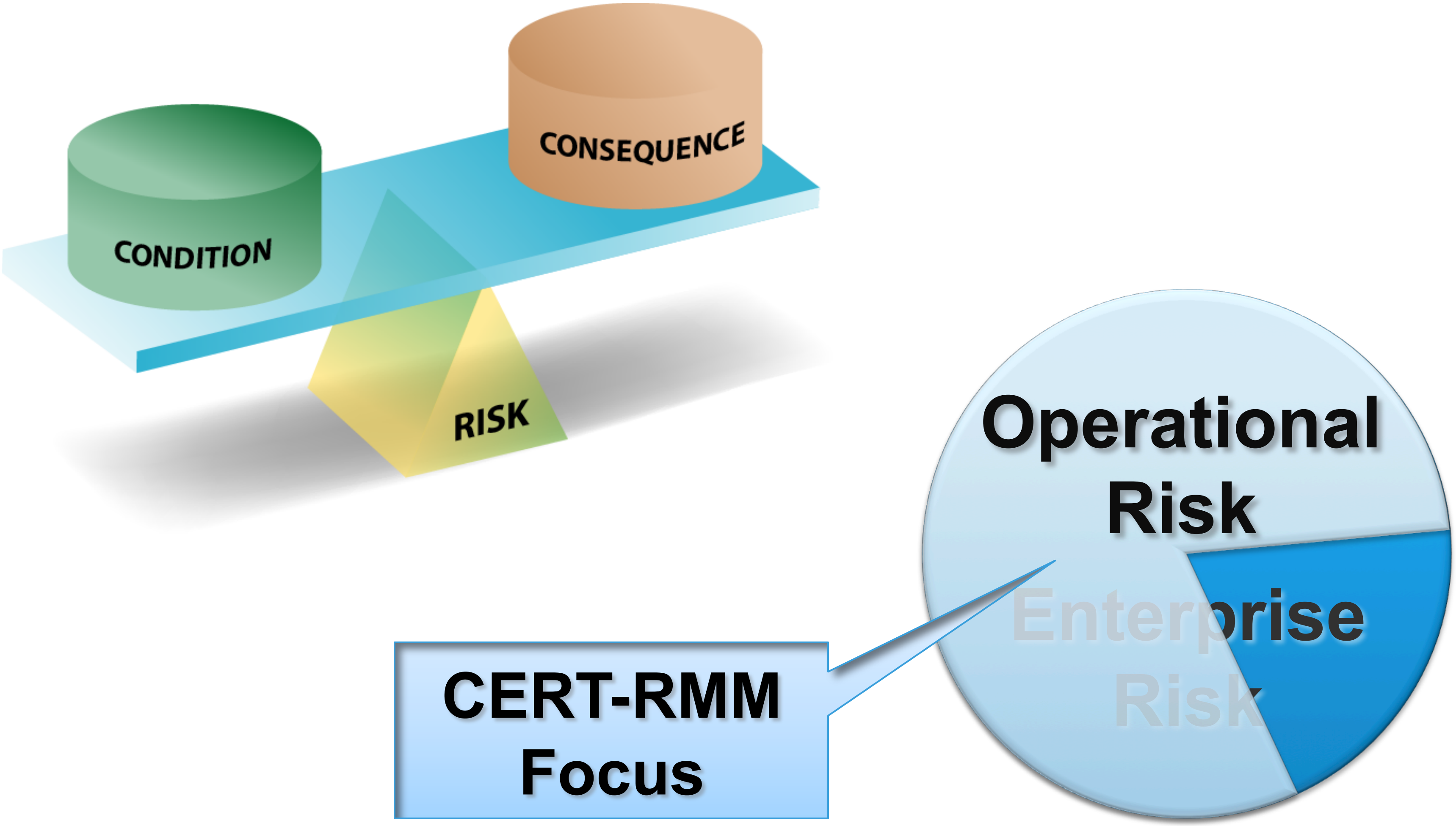
On a minute-to-minute basis, the operational resiliency of the organization is under stress

The stress comes from

- Pervasive use of technology
- Operational complexity
- Movement toward intangible assets
- Global economic pressures
- Open borders
- Geo-political pressures
- Regulatory and legal boundaries
- Legacy issues

This is not an exhaustive list!

Risk



CERT-RMM Focus

Operational risk

A form of risk affecting day-to-day operations

Scope of operational risk is vast, includes:

Deliberate or inadvertent actions of people

Systems & technology failures

Failed internal processes

External events

Challenges for the organization

Meet mission ***no-matter-what***

Cope with operational risk and minimize impact

Move all operational risk management activities in the same direction

Optimize cost/effectiveness

Find meaningful ways to determine (measure) how you're performing ***before*** you're stressed or fail

Building blocks

Adopting a “resiliency” attitude

Fundamental concepts in the solution

Resiliency defined

The principle of convergence

Assuring the mission of services

Relationship of assets to services

An asset view of operational resiliency

The success pyramid

Managing operational resiliency

Resiliency defined

The physical property of a material when it 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** when it **continues to carry out its mission** after **disruption** that **does not push it beyond** its **operational** limit*

What can cause such a **disruption**? Realized risk.

The principle of convergence

A fundamental concept in managing operational resiliency

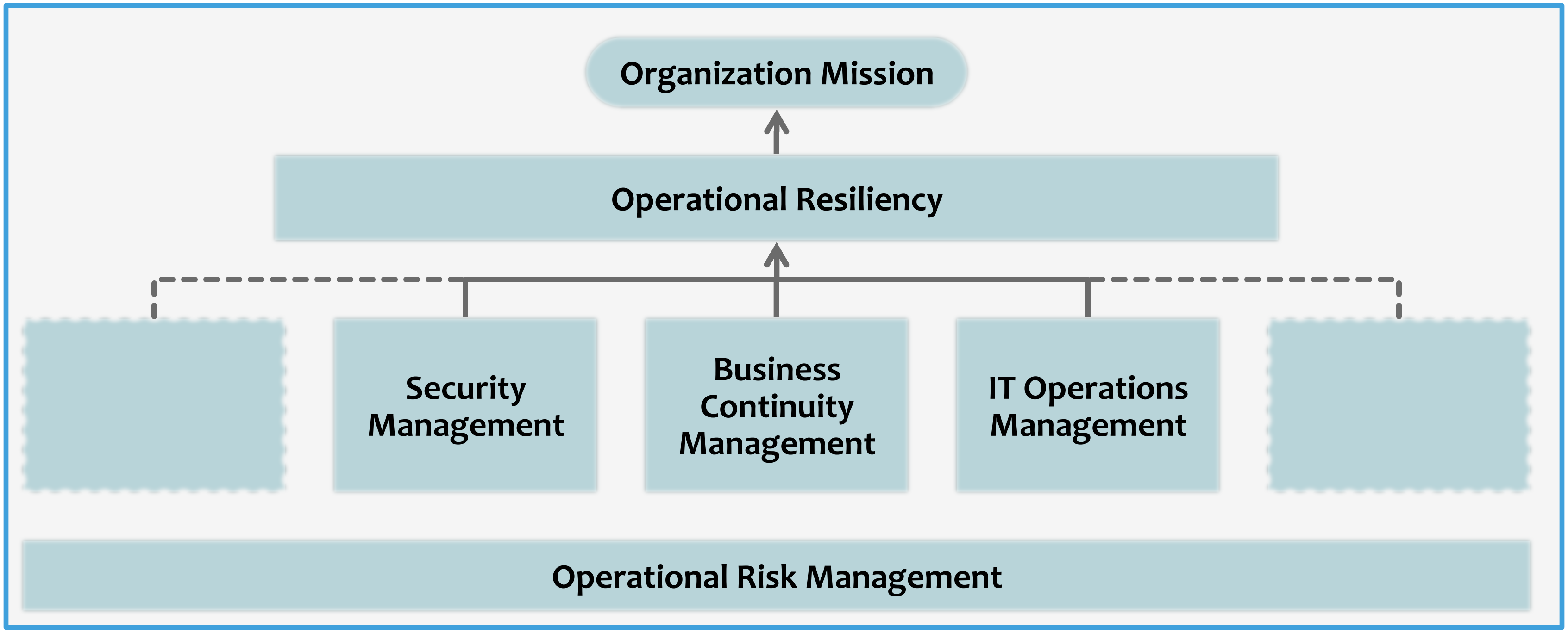
Refers to the harmonization of **operational risk management activities** that have similar objectives and outcomes

Operational risk management activities include

- Security planning and management
- Business continuity and disaster recovery
- I/T operations and service delivery management

Other support activities may also be involved—communications, financial management, etc.

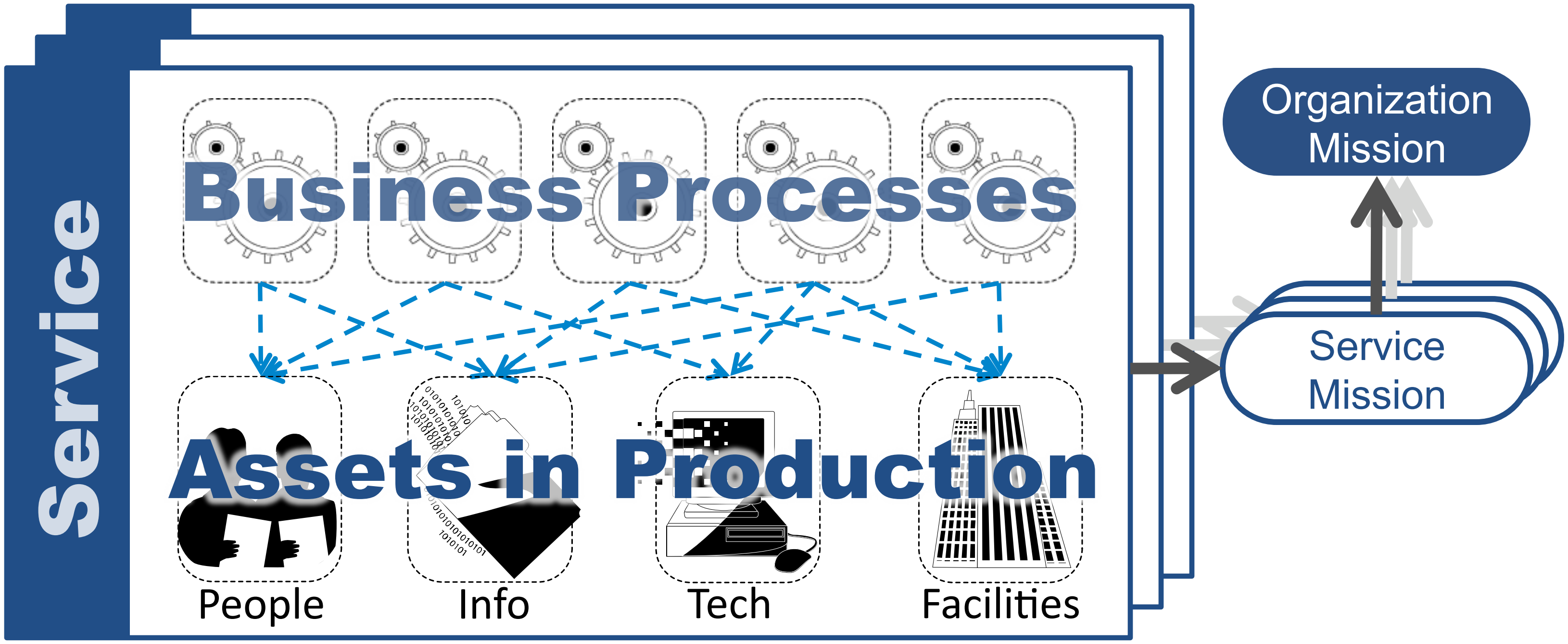
Operational resiliency and convergence



Convergence directly affects the level of operational resiliency

Level of operational resiliency affects ability to meet organizational mission

Organizational context

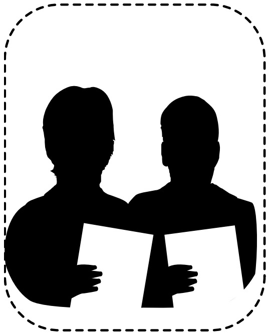


The organization meets its mission when high-value services in the organization meet their missions.

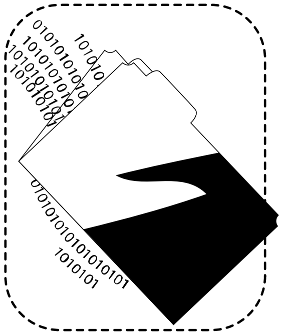
Assets

Something of value to the organization

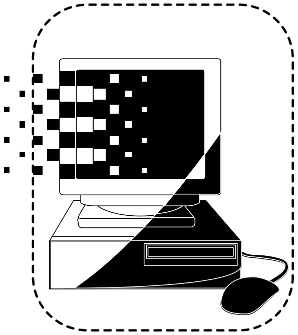
Used by services to meet their mission



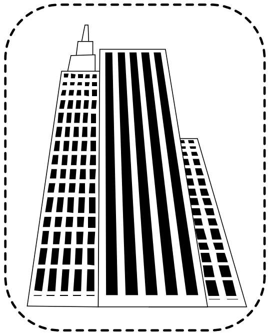
People



Information

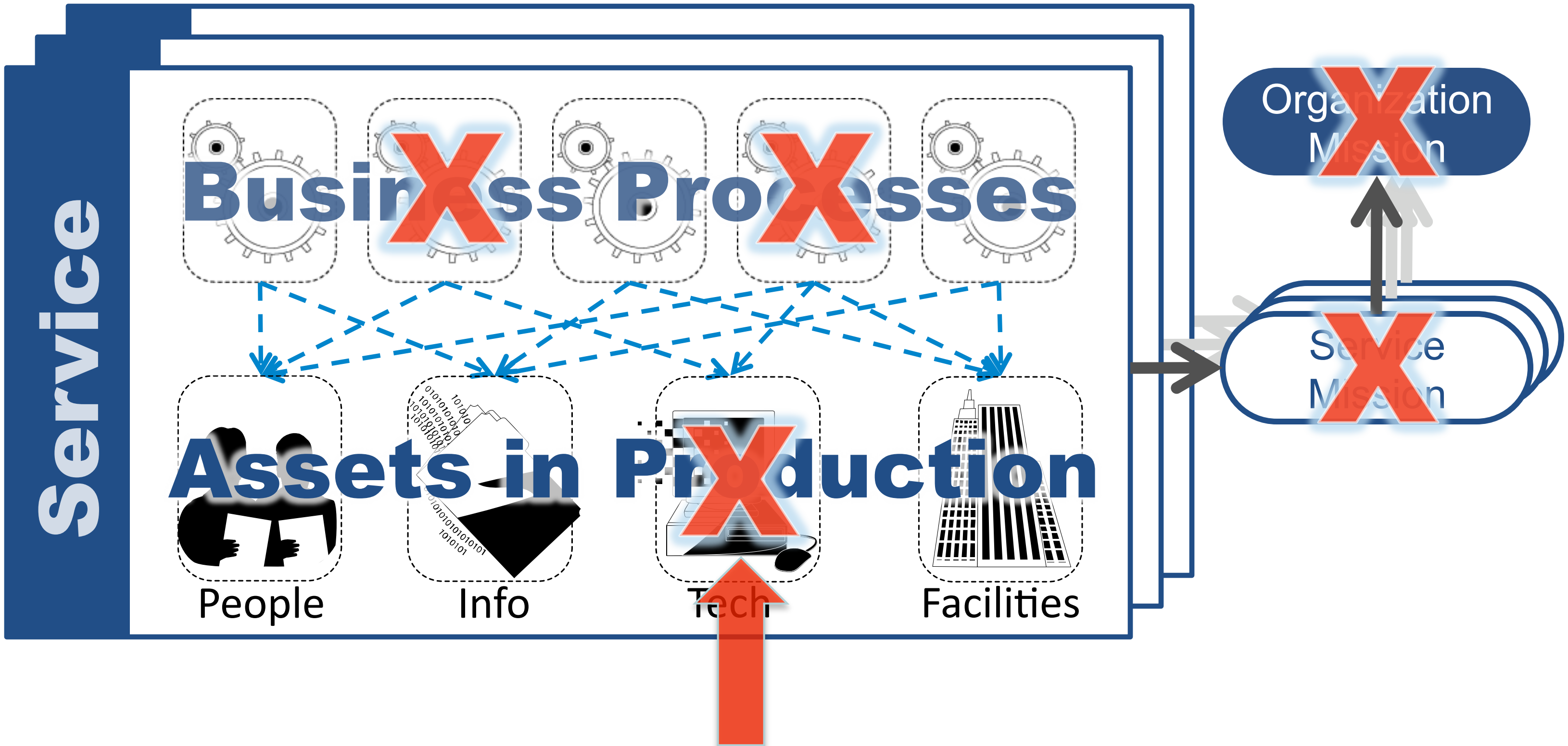


Technology



Facilities

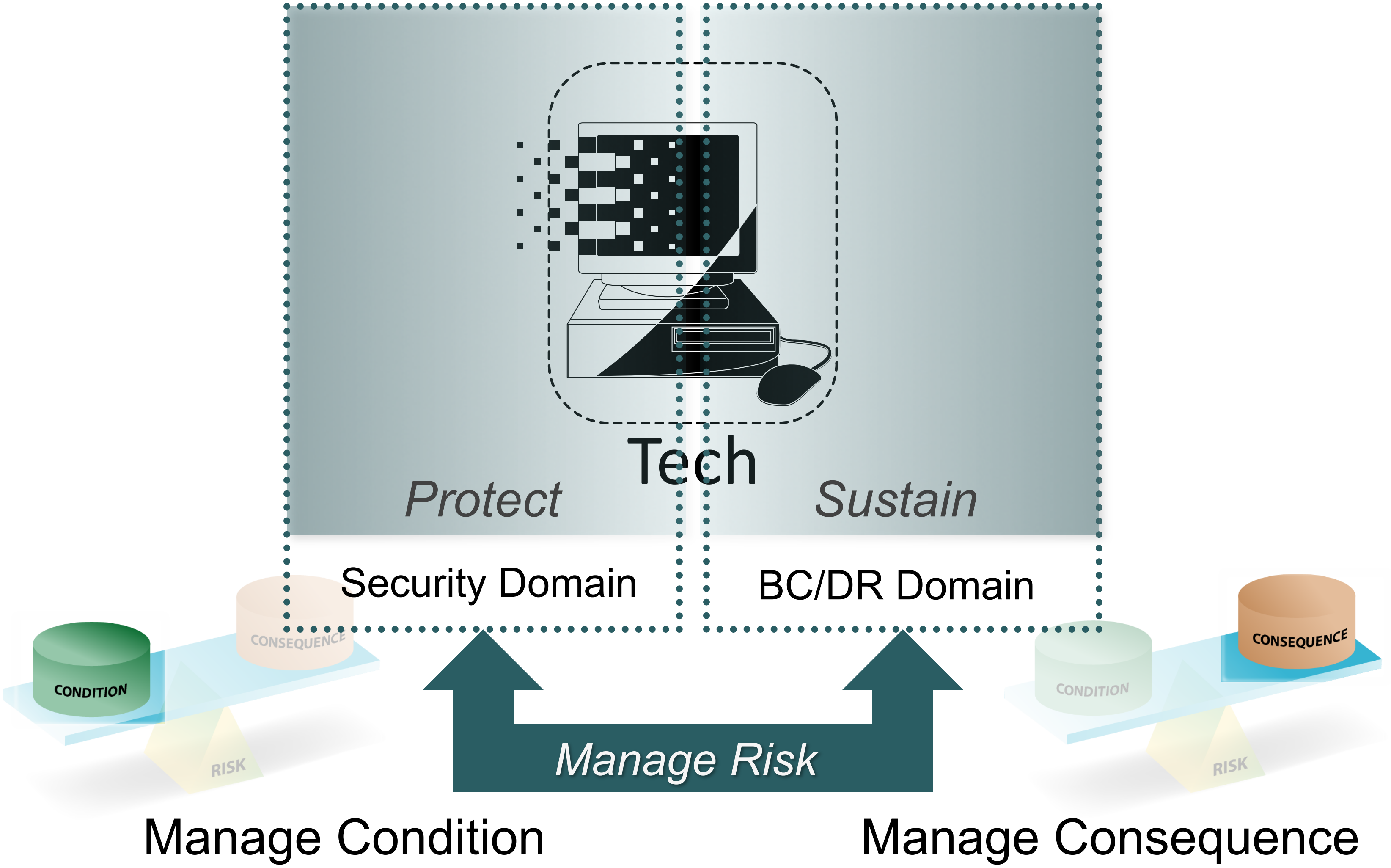
Organizational context - disruption



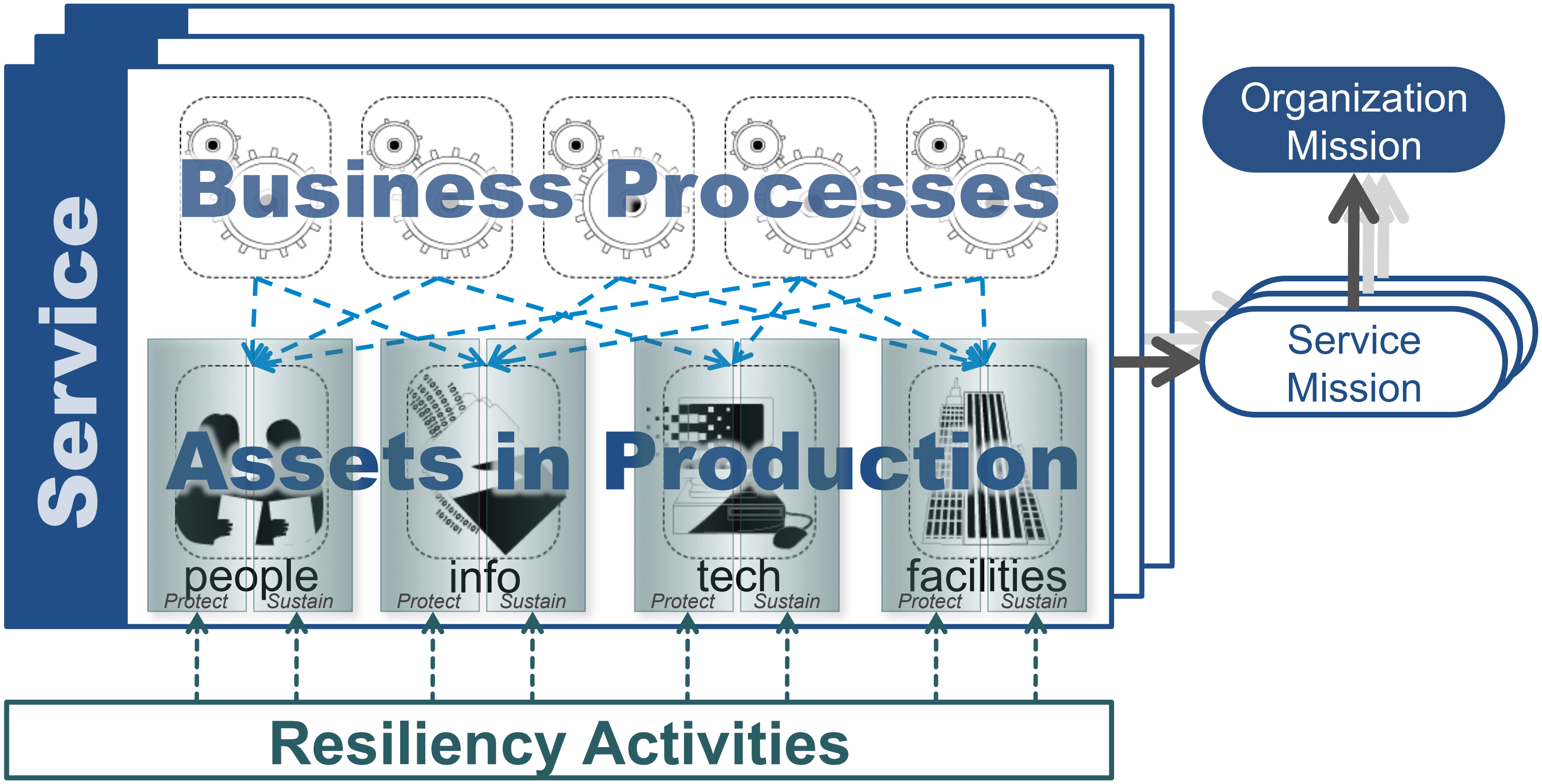
Operational risk can disrupt an asset

And lead to organizational disruption

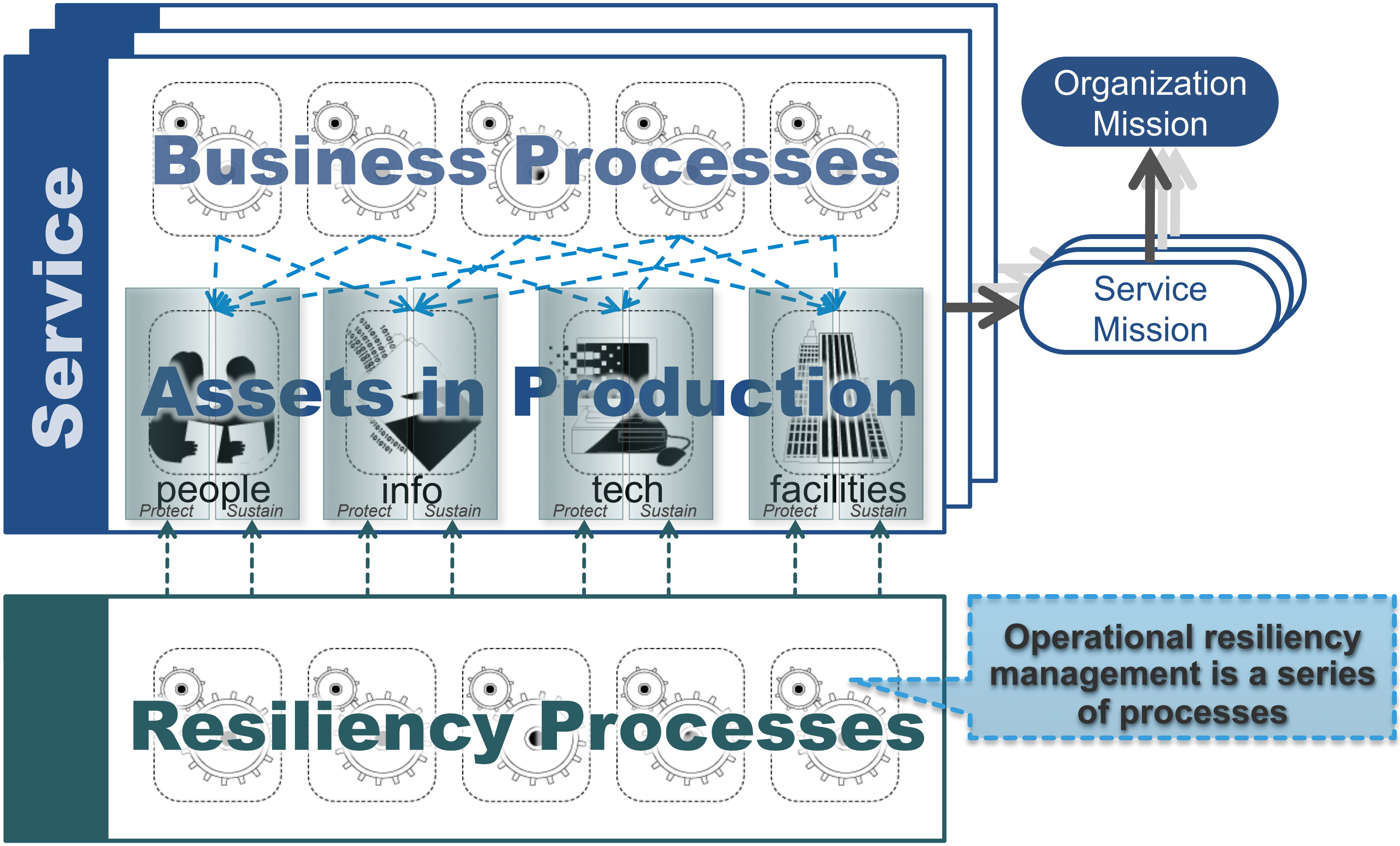
Building resiliency at the asset



Managing operational resiliency -1



Managing operational resiliency -2



Operational resiliency management is a series of processes

The object of improvement -1

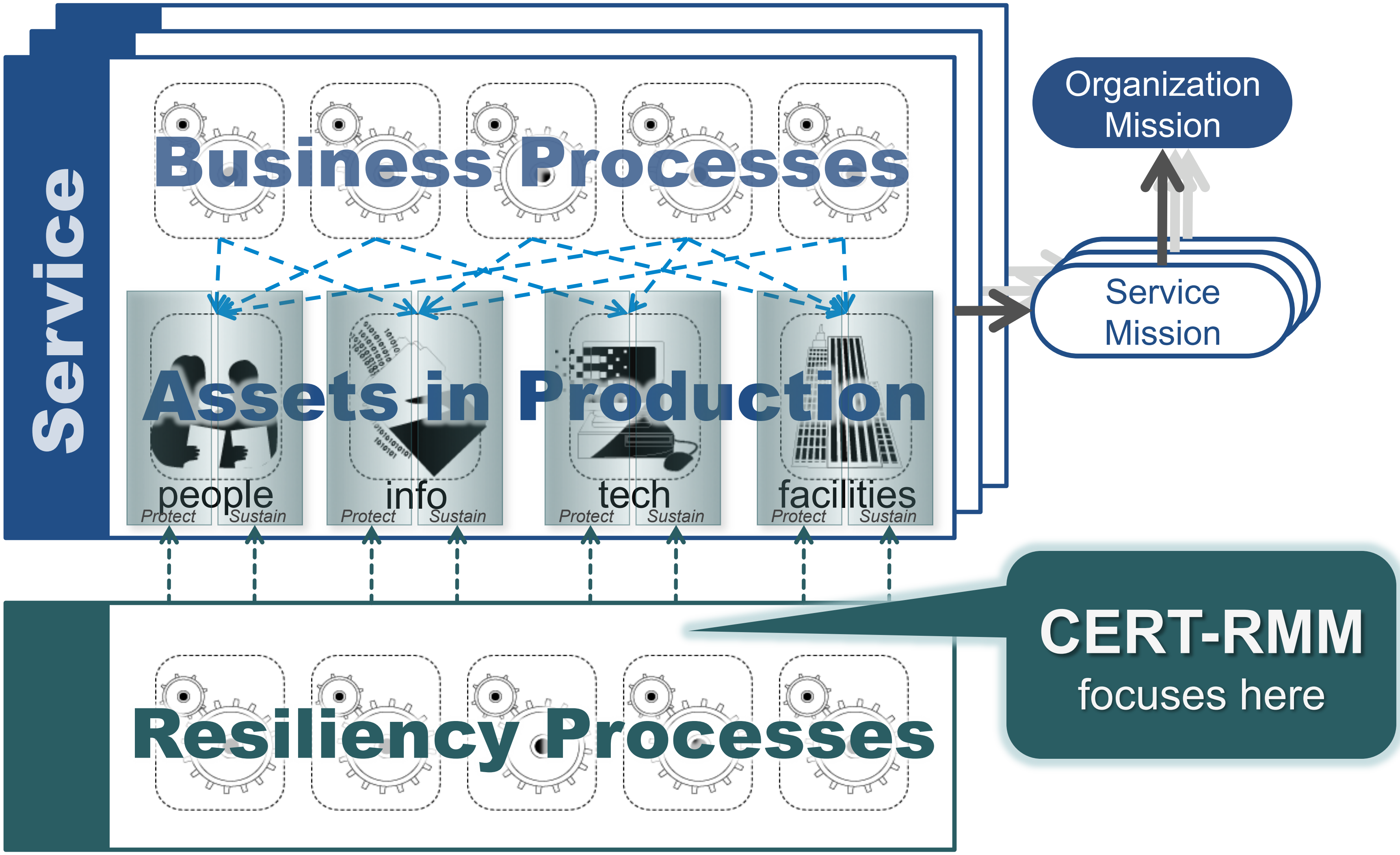
Resiliency processes must also meet their mission→ to ensure that services meet their mission

Ineffective or inconsistent resiliency processes may manifest in diminished service resiliency

Diminished service resiliency makes the mission of the organization vulnerable

The CERT® Resiliency Management Model is focused on ensuring high quality resiliency processes to enable high quality service resiliency ***and support high quality service delivery***

The object of improvement -2



CERT-RMM

Improving services by improving resiliency processes

Why do we need CERT-RMM?

Use “process” as the glue

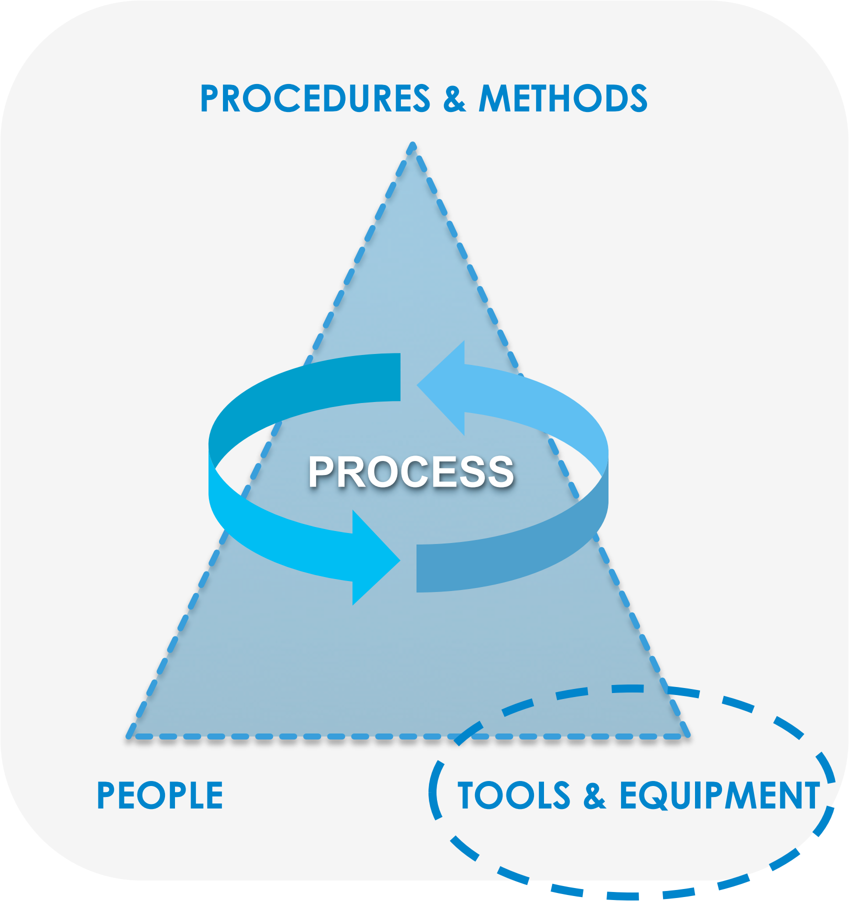
Use process to compliment practices

Focus on stabilizing processes to meet operational resiliency objectives

“Manage your way through” changing risk conditions

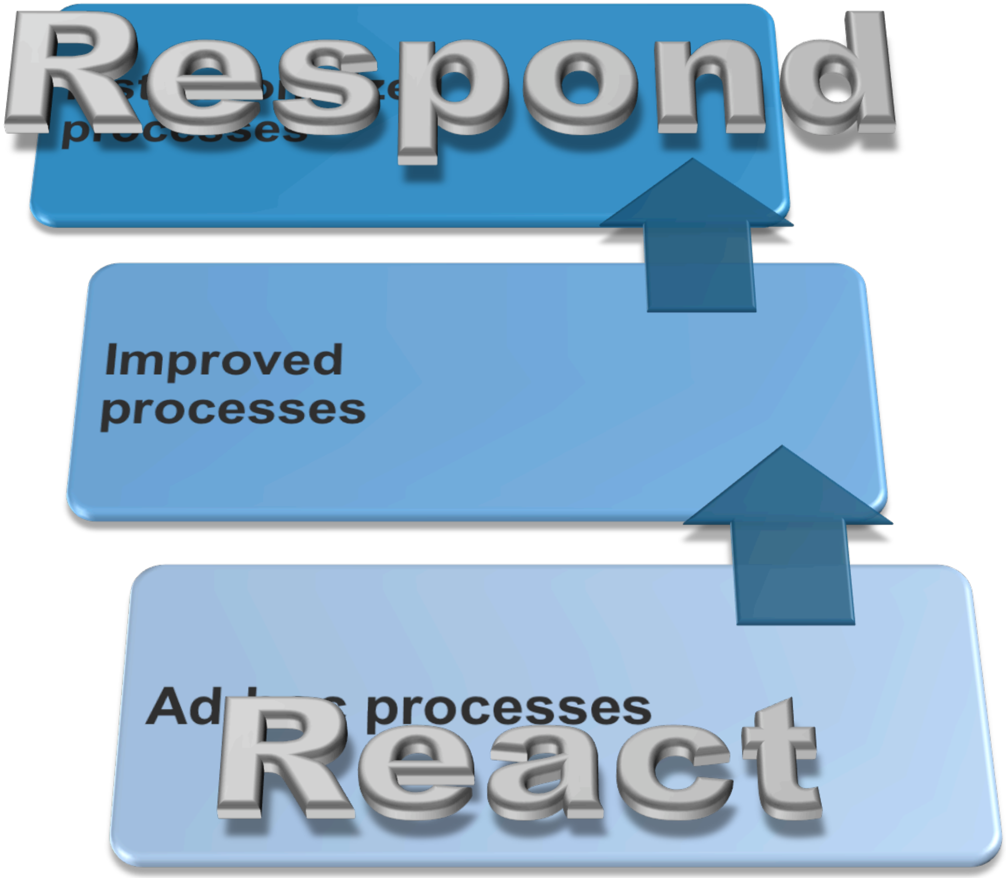
Make your performance more predictable under times of stress

Be able to diagnose where processes are ineffective and fix them before being tested



Operational resiliency is never *solved*—it must be continually managed!

Process institutionalization matters!



Institutionalization improves

- Predictability
- Sustainability
- Consistency
- Stability

These “ilities” are at the heart of the resiliency challenge

Institutionalized operational resiliency processes = more stable, sustainable, consistent, and predictable services

Value of the process capability dimension

Process capability is a measure of institutionalization

The capability dimension can help to answer several important questions in managing operational resiliency:

- How well are we performing today?
- Can we repeat our successes?
- Do we consistently produce expected results?
- Can we adapt seamlessly to changing risk environments?
- Are our processes stable enough to depend on them under times of stress?
- Can we predict how we will perform under times of stress?

You need to know not only that you're doing the right things but that you are doing them in a sustainable way.

CERT® Resiliency Management Model

A capability-focused model—guidelines and practices for

- Converging of security, business continuity, and IT ops activities
- Measuring and maturing these activities

Focuses on “what” not “how”

Organized into 26 process areas

Provides 4-level capability dimension

Common vernacular and basis for objective appraisals

www.cert.org/resiliency

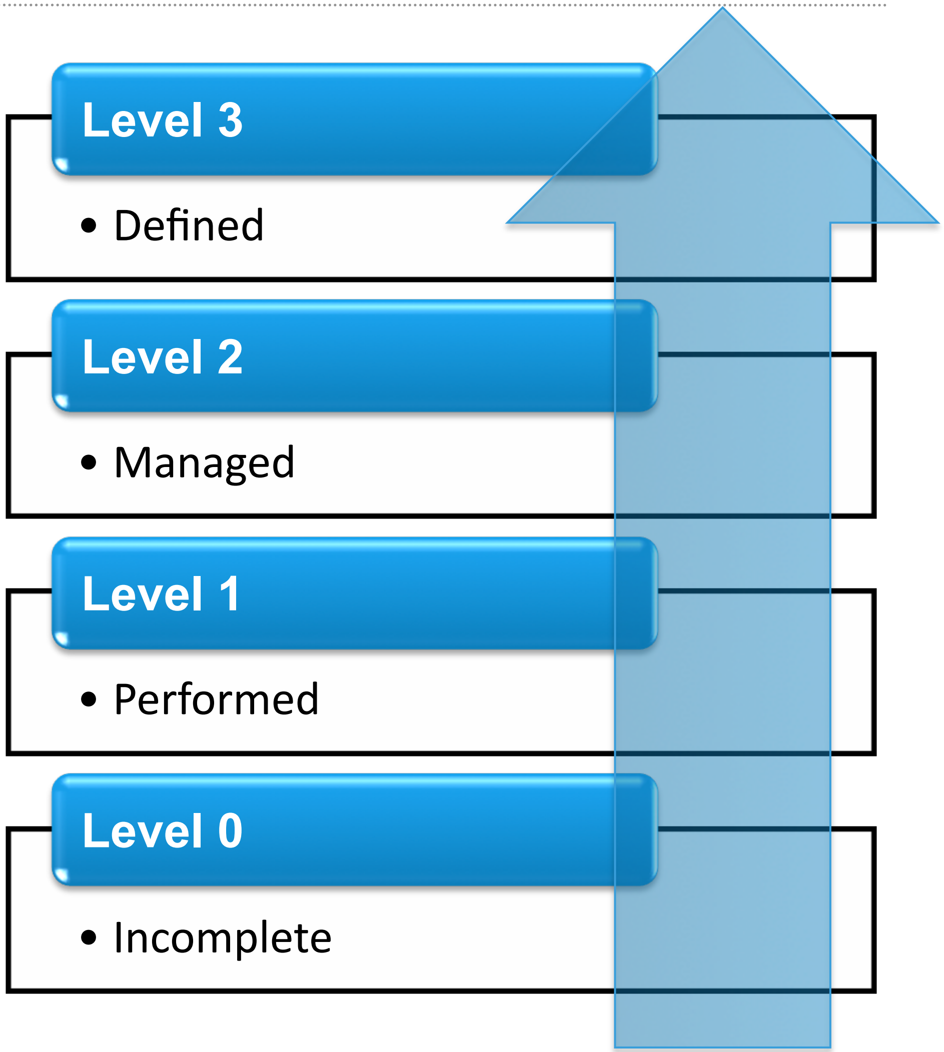
RMM capability levels

Apply to each process area, independently

Indicate extent to which the activities in the process area are

- Being performed (level 1)
- Institutionalized (levels 2 and 3)

Model provides detailed guidance on achieving these levels



Level 3

- Defined

Level 2

- Managed

Level 1

- Performed

Level 0

- Incomplete

CERT-RMM by the numbers

4
Process Categories

26
Process Areas

256
Specific Practices

94
Specific Goals

260
L2 Generic Practices

52
L3 Generic Practices

RMM at a glance

26 Process Areas in 4 categories

Engineering

ADM	Asset Definition and Management
CTRL	Controls Management
RRD	Resiliency Requirements Development
RRM	Resiliency 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

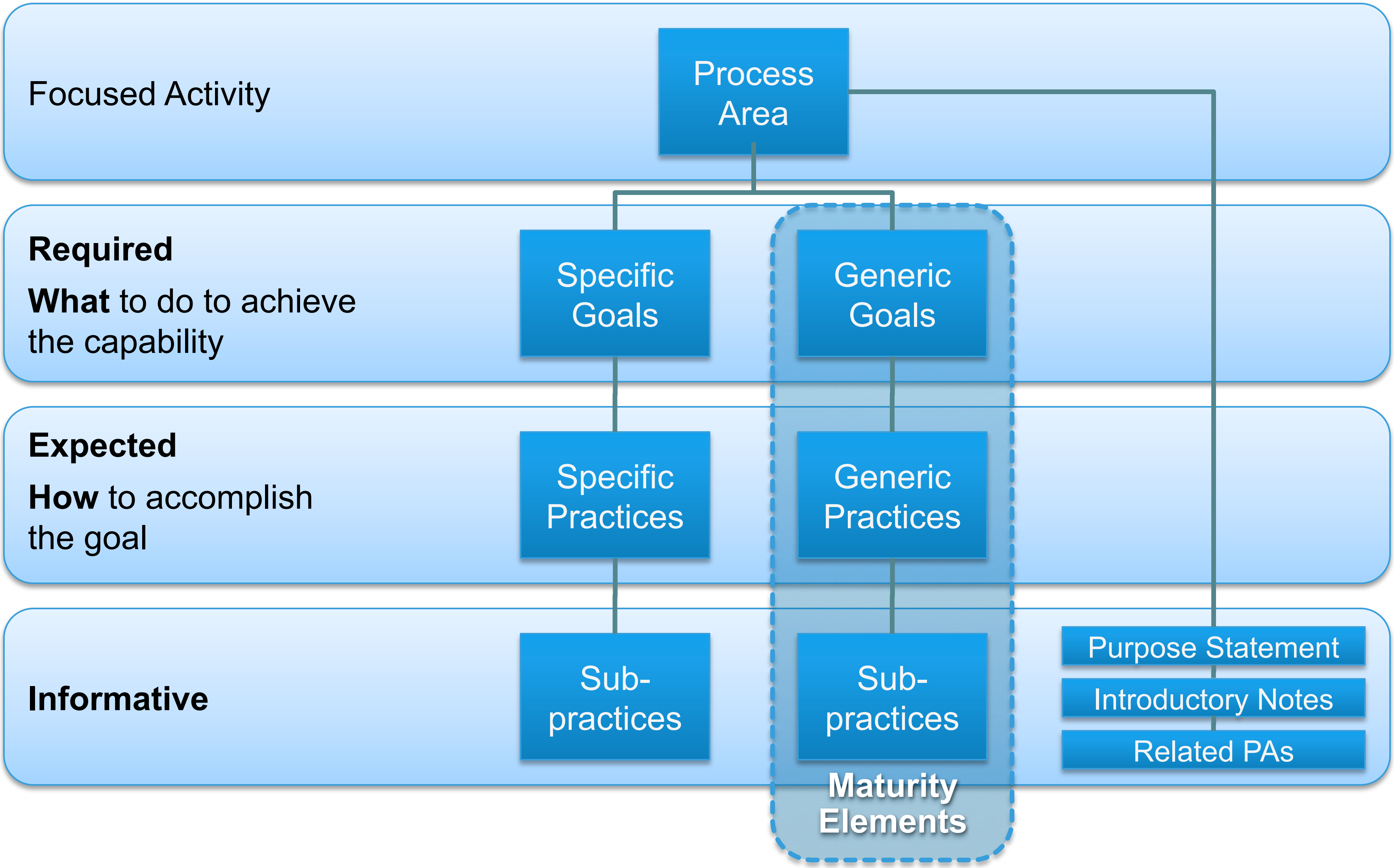
Operations Management

AM	Access Management
EC	Environmental Control
EXD	External Dependencies Management
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 area structure



Using CERT-RMM

Deploying CERT-RMM for improved practices and extending process improvement capabilities

Using CERT-RMM

CERT-RMM can be used as a

- Starting point for leveraging convergence across security, business continuity, and IT operations activities
- Reference model for understanding the scope of managing operational resiliency
- Taxonomy to enable internal and external communication
- Organizing construct for codes of practice, standards, and regulations and a framework for compliance
- Process improvement model to catalyze improvement efforts
- Baseline for appraising an organization’s capability
- Guide for improvement in areas where an organization’s capability does not equal its desired state

CERT-RMM coverage of codes of practice

Currently mapped to CERT-RMM:

- BS25999-1:2006
- CMMI v1.2
- CMMI for Services
- CobiT 4.1
- COSO ERM
- DRII GAP
- FFIEC Handbooks (Security, BCP)
- ISO 20000-1:2005(E)
- ISO 20000-2:2005(E)
- ISO 24762:2008(E)
- ISO 27002:2005
- NFPA 1600 (2007)
- PCI DSS v1.1
- Val-IT

In progress or consideration:

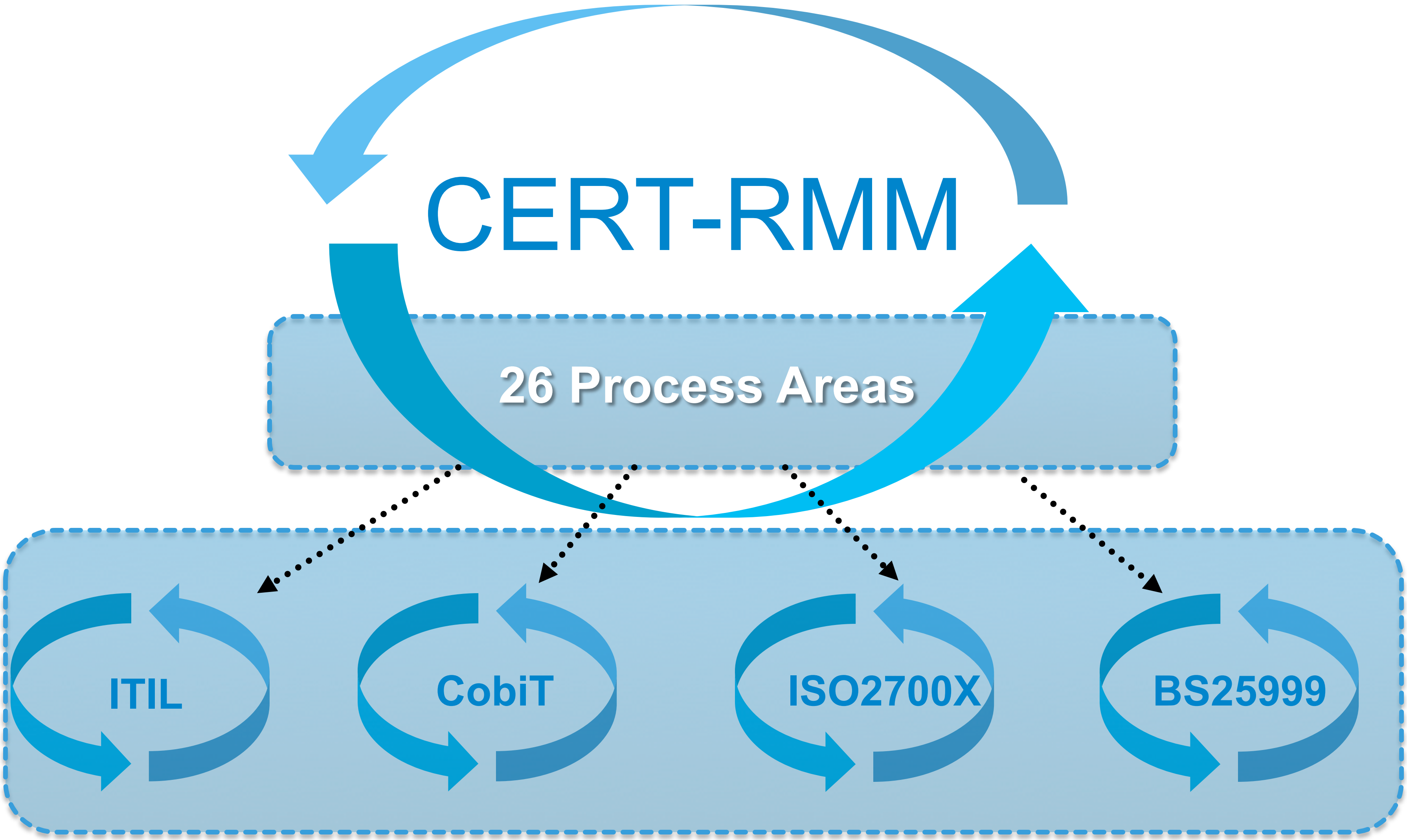
ISO SE7 Application Security Std

HR1-Title 9 Voluntary Standard (TBD)

NIST standards/FISMA provisions

Documented in the REF Code of Practice Crosswalk, v0.95R to be updated with release of RMM version 1.0

Example: CERT-RMM as an organizing principle



CERT-RMM

26 Process Areas

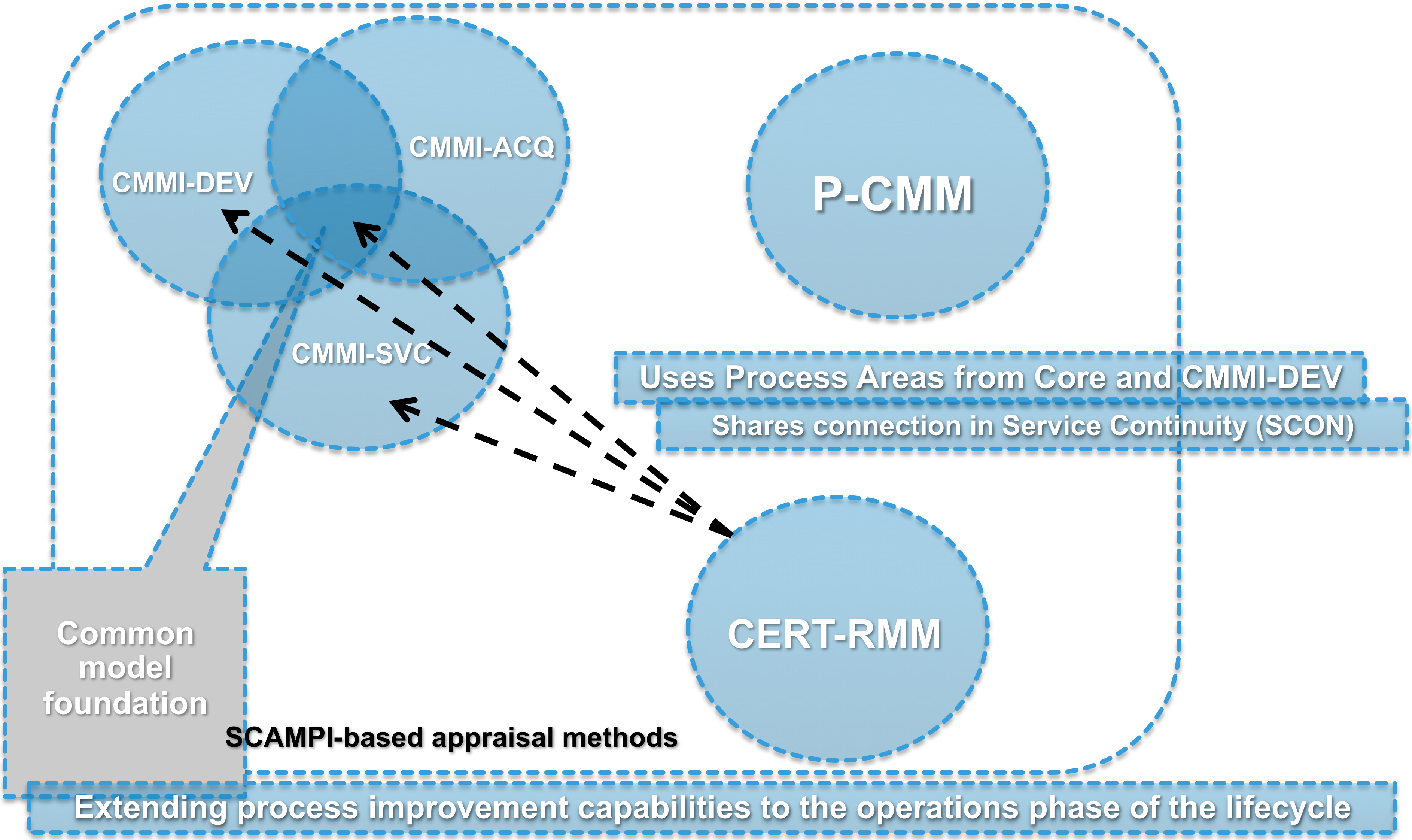
ITIL

CobiT

ISO2700X

BS25999

Positioning CERT-RMM in CMMI



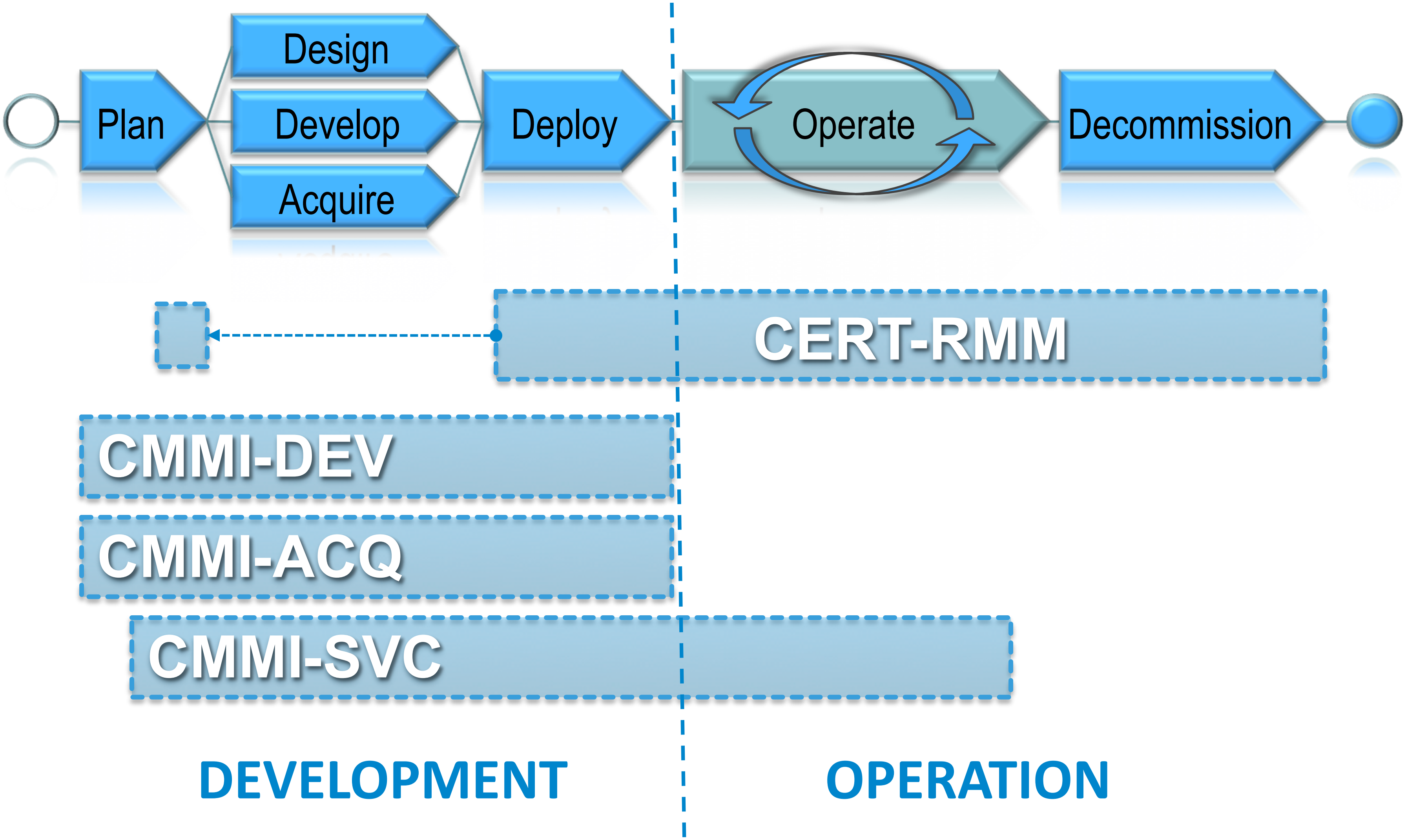
Uses Process Areas from Core and CMMI-DEV

Shares connection in Service Continuity (SCON)

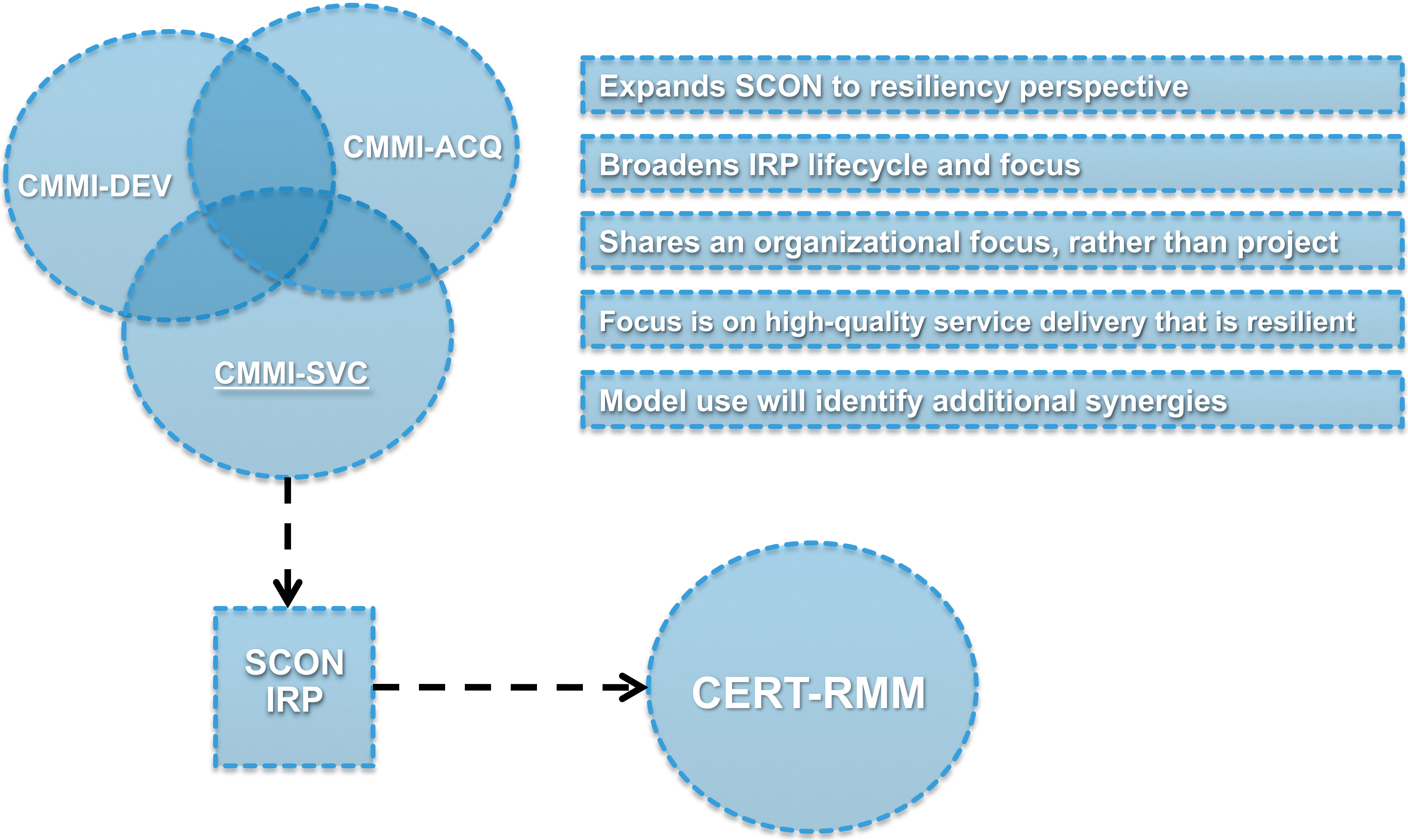
SCAMPI-based appraisal methods

Extending process improvement capabilities to the operations phase of the lifecycle

CERT-RMM position in lifecycle



CERT-RMM and CMMI-SVC



Expands SCON to resiliency perspective

Broadens IRP lifecycle and focus

Shares an organizational focus, rather than project

Focus is on high-quality service delivery that is resilient

Model use will identify additional synergies

CERT-RMM activities

Where CERT-RMM is today and where it's going

CERT-RMM current activities

First Class A RMM appraisal recently completed; next appraisal scheduled

First Class C RMM appraisal completed

Working to position RMM for resiliency management and measurement in the civilian agencies

Continuing to support adoption in the financial industry through ongoing benchmarking

Initiating a resiliency measurement and analysis project to develop guidance on measurement and metrics activities in this space

CERT-RMM planned activities

CERT-RMM “official” version 1.0 (Technical Report)

CERT-RMM Addison-Wesley Book, August 2010

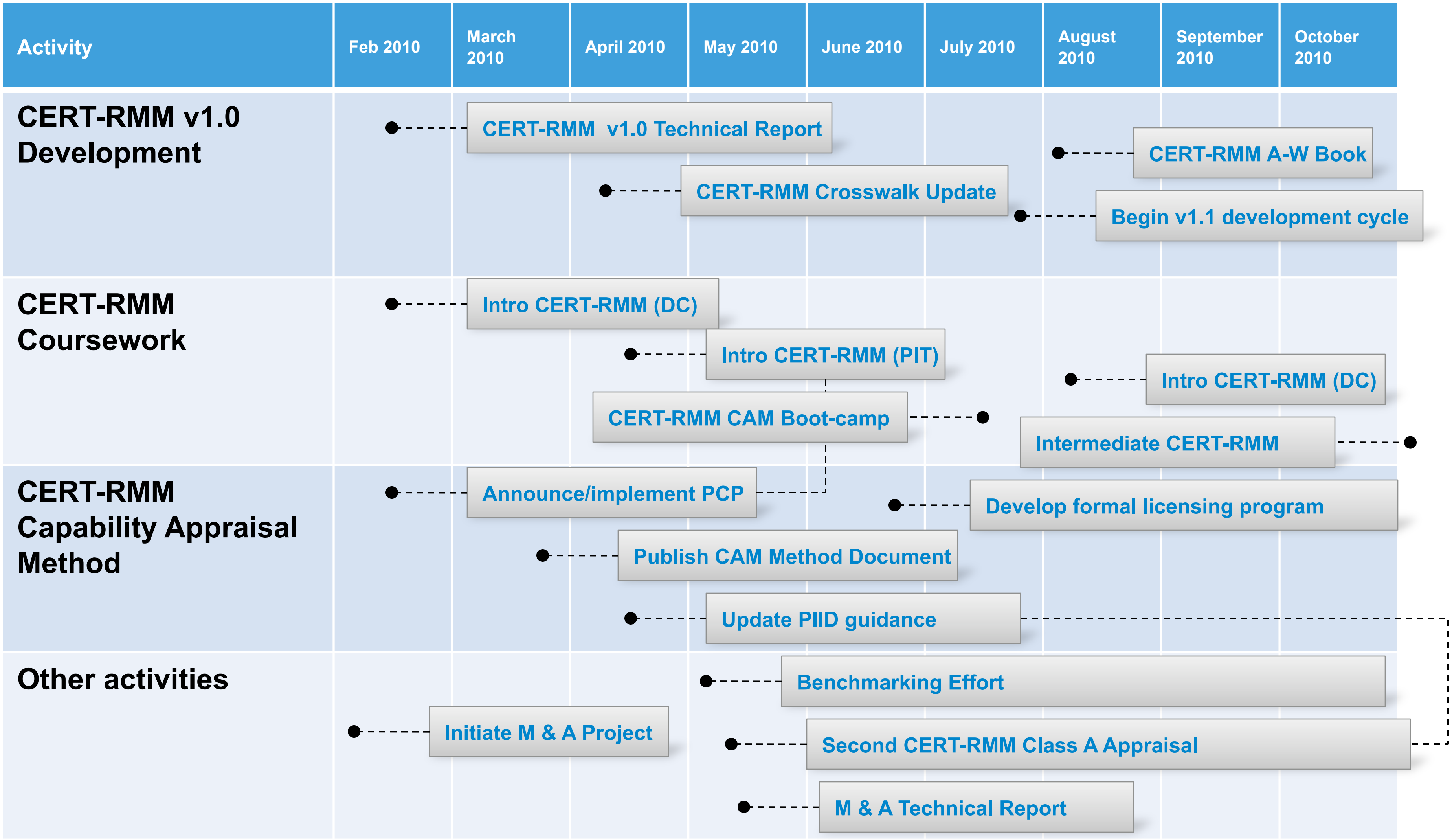
Licensing program for course and appraisal

- Provisional certification program appraisers
- Instructor apprentice program

CERT-RMM Appraisal Bootcamp

Formal appraisal guidance and method definition document development

CERT-RMM FY2010 Timeline



Activity | Feb 2010 | March 2010 | April 2010 | May 2010 | June 2010 | July 2010 | August 2010 | September 2010 | October 2010

CERT-RMM v1.0 Development

- CERT-RMM v1.0 Technical Report
- CERT-RMM Crosswalk Update
- CERT-RMM A-W Book
- Begin v1.1 development cycle

CERT-RMM Coursework

- Intro CERT-RMM (DC)
- Intro CERT-RMM (PIT)
- CERT-RMM CAM Boot-camp
- Intro CERT-RMM (DC)
- Intermediate CERT-RMM

CERT-RMM Capability Appraisal Method

- Announce/implement PCP
- Publish CAM Method Document
- Update PIID guidance
- Develop formal licensing program

Other activities

- Initiate M & A Project
- Benchmarking Effort
- Second CERT-RMM Class A Appraisal
- M & A Technical Report

RMM support available from CERT

Introductory course, public and onsite offerings – immediate

Workshops and executive briefings – immediate

Improvement programs (appraisal plus improvement planning and coaching) – immediate

Appraisals (class A, B, and C) – immediate

Users group at CERT – 2010

Advanced courses (intermediate, appraiser) – 2010

Licensing (appraisal and intro course) – 2010

RMM Project Team and Contacts

Rich Caralli
RMM Architect and Lead Developer
rcaralli@cert.org

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

Kelly Kimberland
Public Relations — All Media Inquiries
public-relations@sei.cmu.edu

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

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

Julia Allen
RMM Developer
jha@sei.cmu.edu

SEI Customer Relations
customer-relations@sei.cmu.edu
412-268-5800

www.cert.org/resiliency

Questions?

Notices

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.