Improving Operational Resilience Processes

CERT Resilience Management Model (RMM)

10th Annual CMMI Technology Conference and User Group

Rick Barbour & Rich Caralli
CERT
Software Engineering Institute

Sponsored by the
U.S. Department of Defense

Agenda

- What is CERT®-RMM?
- Risk, Resilience & Convergence
- Overlap between CERT-RMM & CMMI process areas
- CERT-RMM as an organizing principle
- CERT-RMM Current Activities

What is CERT®-RMM?

The CERT® Resilience Management Model (CERT-RMM) is a capability model for managing and improving operational resilience.

- *Positions **operational resilience** in a process improvement view*
- *Includes 26 **"process areas"***
- Focuses on the operations phase of the lifecycle
- Defines "maturity" through "capability levels" consistent with CMMI
- Uses CMMI architecture for ease of adoption
- *Includes a "continuous representation" for agile adoption*

Distinguishing features of CERT®-RMM

CERT-RMM brings several innovative and advantageous concepts to the management of operational resilience.

- ***The convergence advantage:*** *merging the disciplines of security, BC/DR, and IT ops into a single model*
- **The process advantage:** elevating these disciplines to a process view, useful as an integration and measurement framework
- ***The maturity advantage:*** *provides a foundation for practical institutionalization of practices—critical for retaining these practices under times of stress*

CERT-RMM background

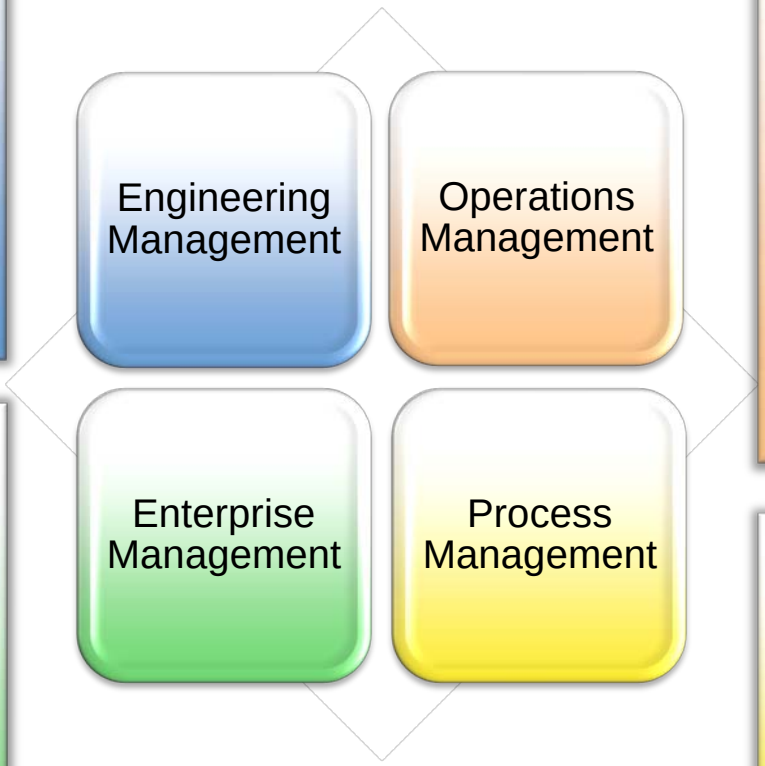
CERT-RMM began as research into the application of process improvement and maturity model approaches to security management.

- Literary review and affinity analysis of over 800 standard practices security, BC/DR, and IT ops communities
- Examination of body of knowledge of high-maturity organizations
- Codification of model using trusted CMMI architecture and concepts
- Benchmarking and piloting in the banking/finance community, defense contractors, and US government federal civilian agencies

CERT-RMM at a glance

Requirements Management
RRD – Resilience Requirements Development
RRM – Resilience Requirements Management
Asset Management
ADM – Asset Definition and Management
Establishing Resilience
SC – Service Continuity
CTRL – Controls Management
RTSE – Resilient Technical Solution Engineering

Governance, Risk, & Compliance
COMP – Compliance
EF – Enterprise Focus
RISK – Risk Management
Supporting Resilience
COMM – Communications
FRM – Financial Resource Management
HRM – Human Resource Management
OTA – Organizational Training & Awareness



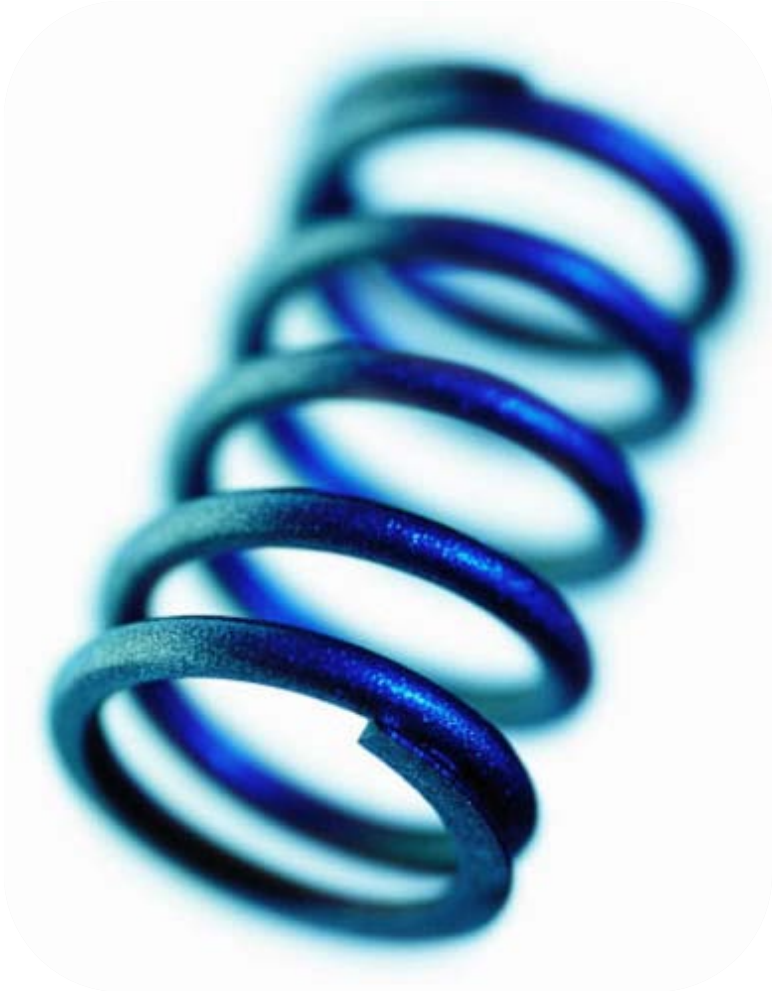
Asset Resilience Management
EC – Environmental Control
KIM – Knowledge & Information Management
PM – People Management
TM – Technology Management
Sourcing
EXD – External Dependencies
Threat, Incident, & Access Management
AM – Access Management
ID – Identity Management
IMC – Incident Management & Control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

Data Collection & Logging
MON – Monitoring
Process Management
MA – Measurement and Analysis
OPD – Organizational Process Definition
OPF – Organizational Process Focus

Resilience, Convergence & Risk

Operational resilience

Resilience: 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]



Operational resilience: *The* ***emergent*** *property of an* ***organization*** *exhibited when it* ***continues to carry out its mission*** *after* ***disruption*** *that* ***does not push it beyond*** *its* ***operational*** *limit*

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

- 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.

Operational resilience & operational risk

Security and business continuity are not end-states; they are continuous processes

Effective operational risk management requires harmonization: convergence of these activities working toward the same goals

Operational resilience emerges from effective **operational risk management**

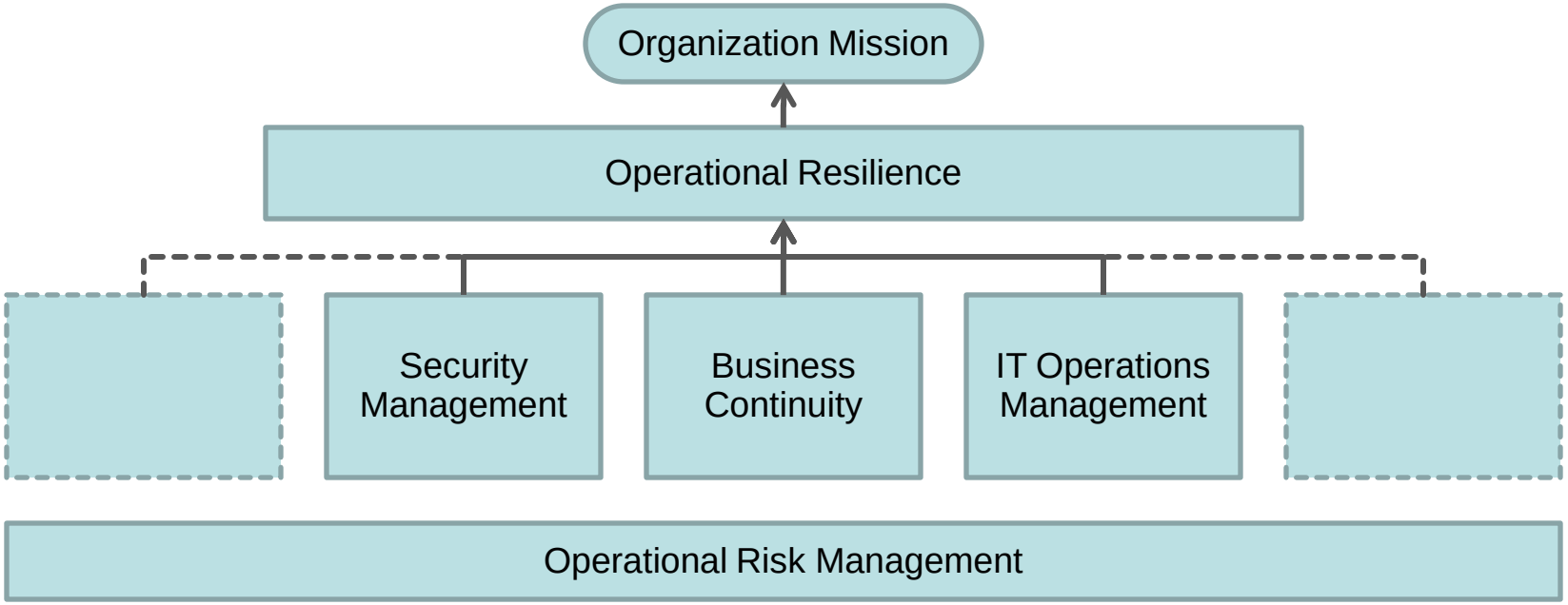
Actions of people

Systems & technology failures

Failed internal processes

External events

Operational resilience and convergence

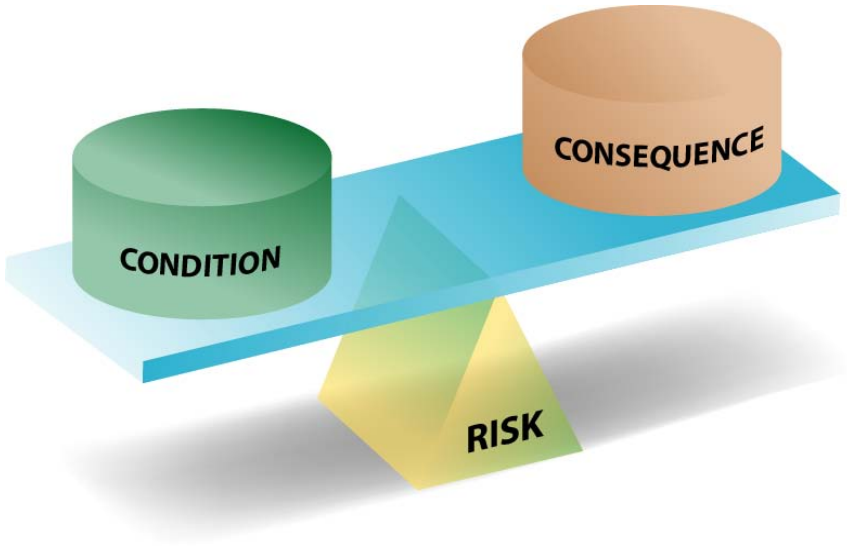


Convergence directly affects the level of operational resilience.

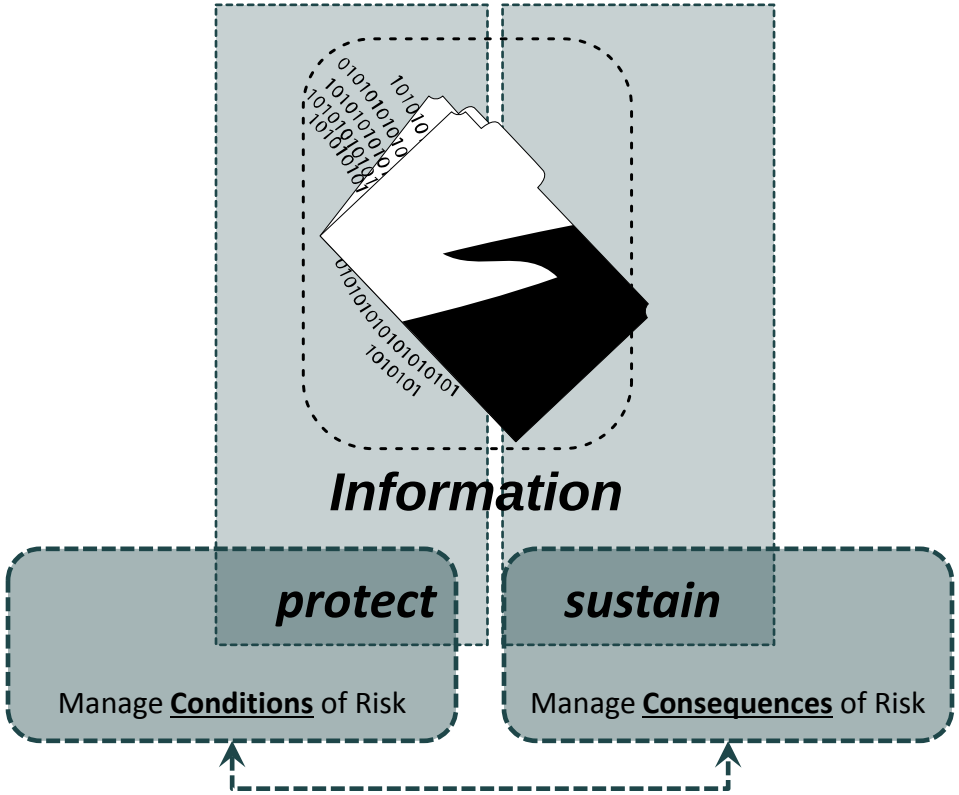
Level of operational resilience affects the ability to meet organizational mission.

Protection, sustainability, and risk

Basic risk equation

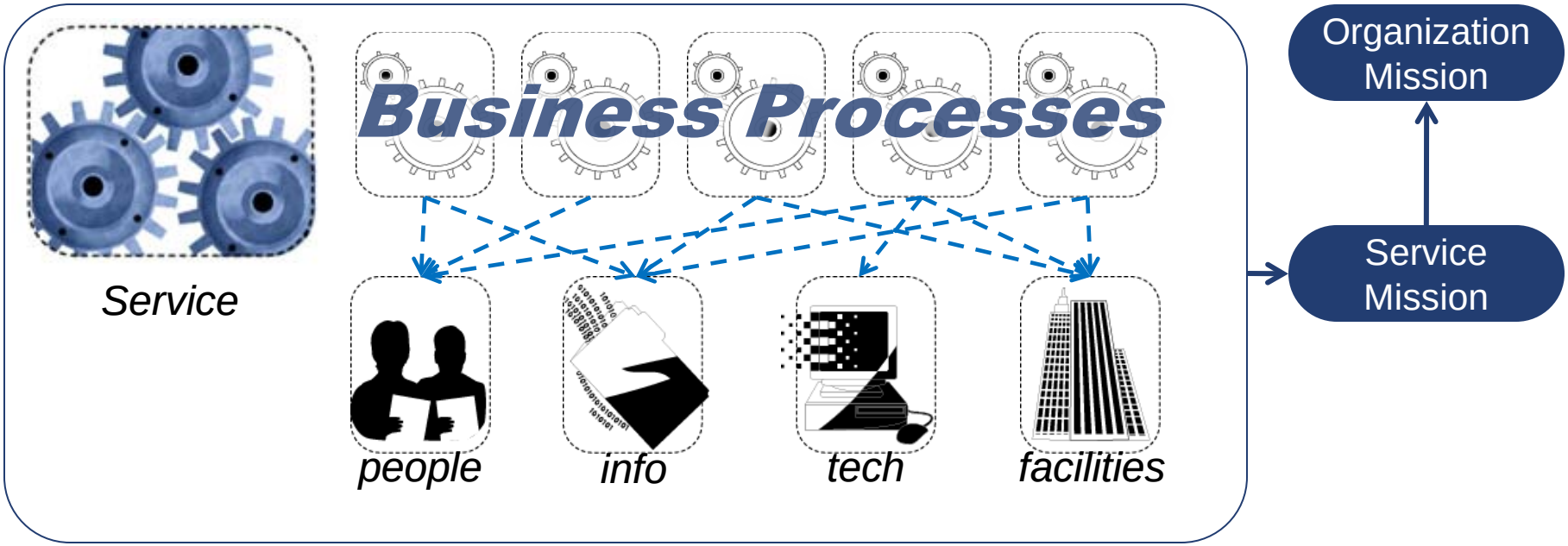


Protection & sustainability



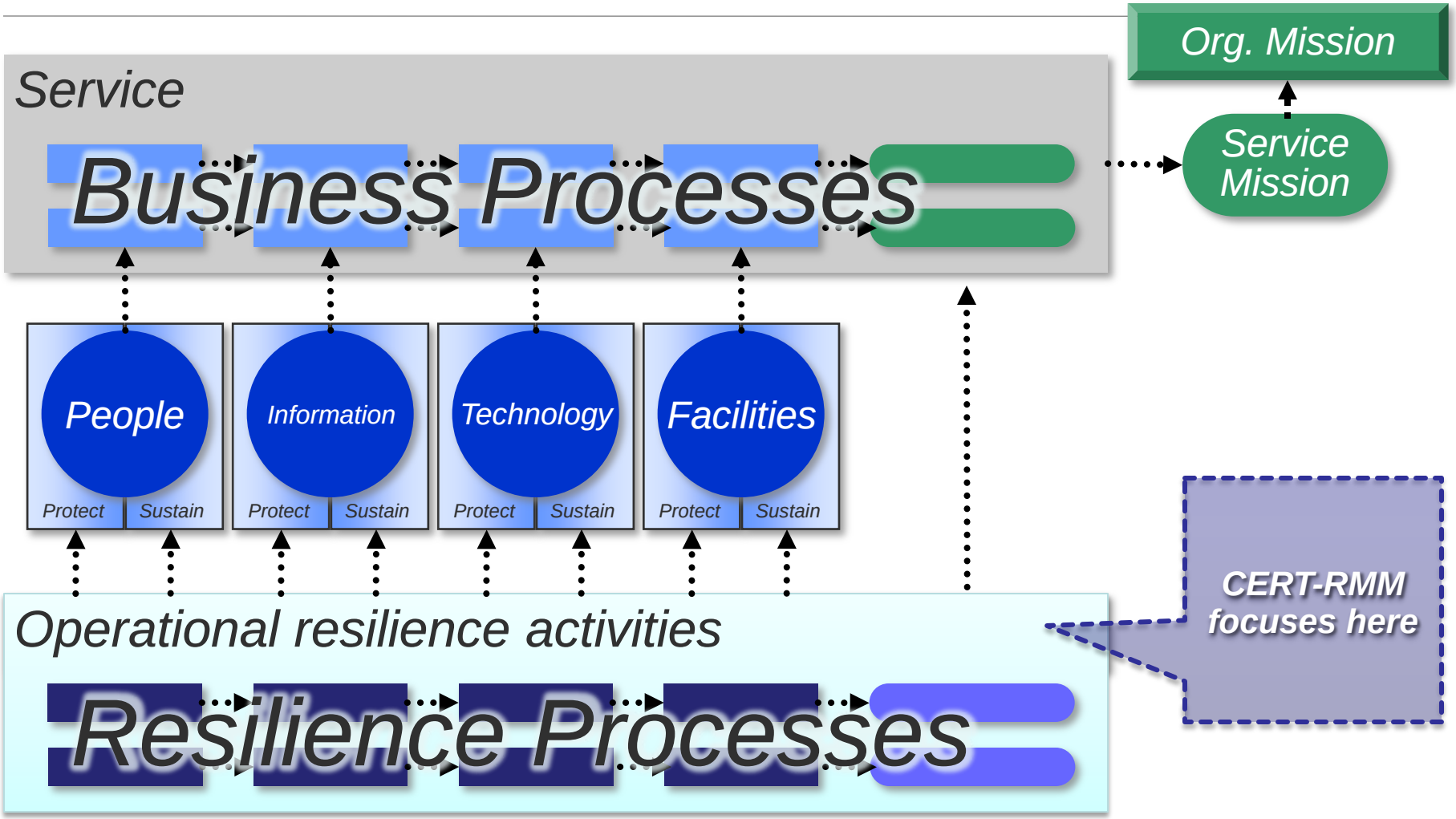
Operational resilience requires ***optimizing*** these strategies in a way that minimizes operational risk (to the associated services) and *is resource efficient:* ***the management challenge of operational resilience.***

A service view

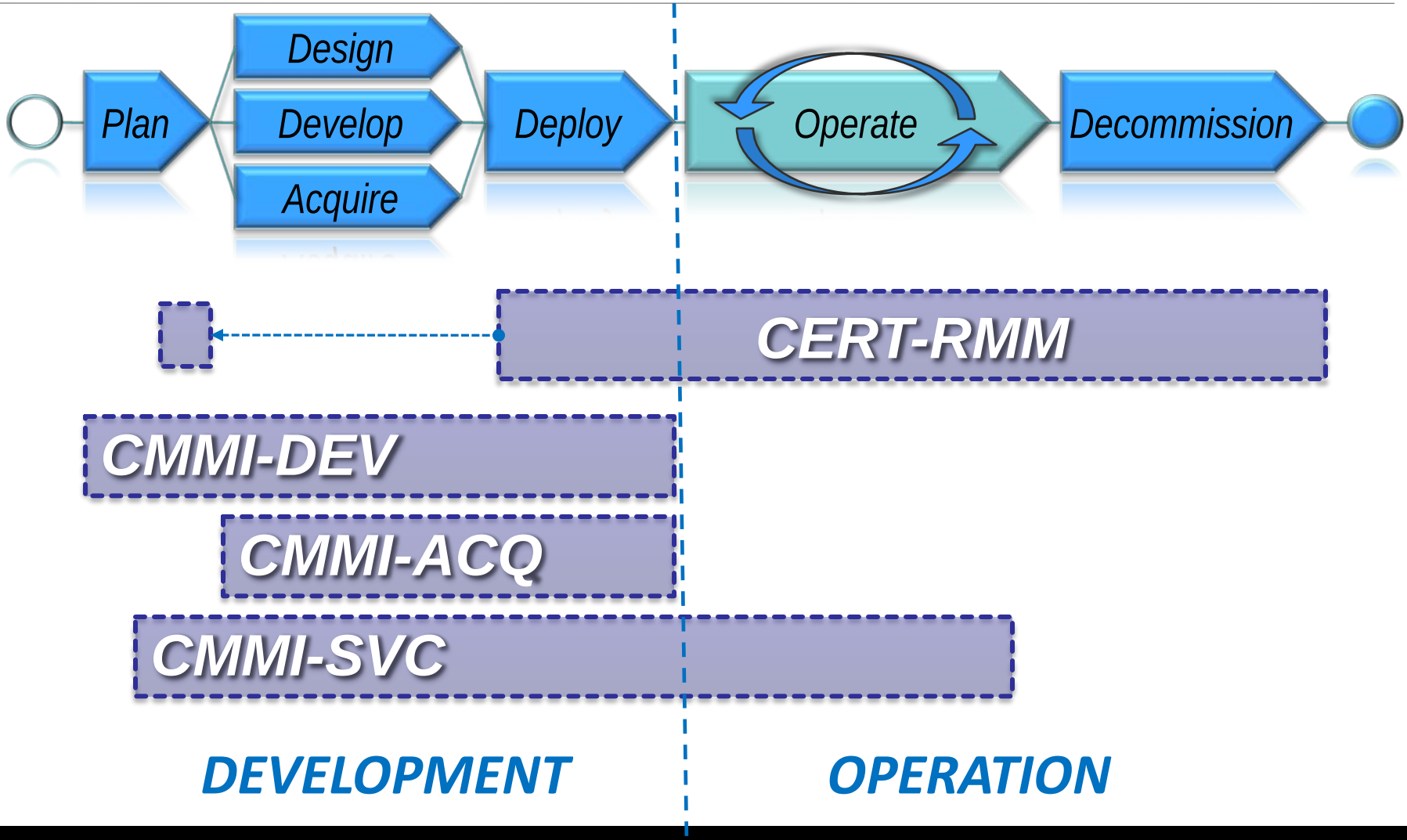


The organization meets its mission when high-value services in the organization meet their missions.

The object of improvement



CERT-RMM position in lifecycle



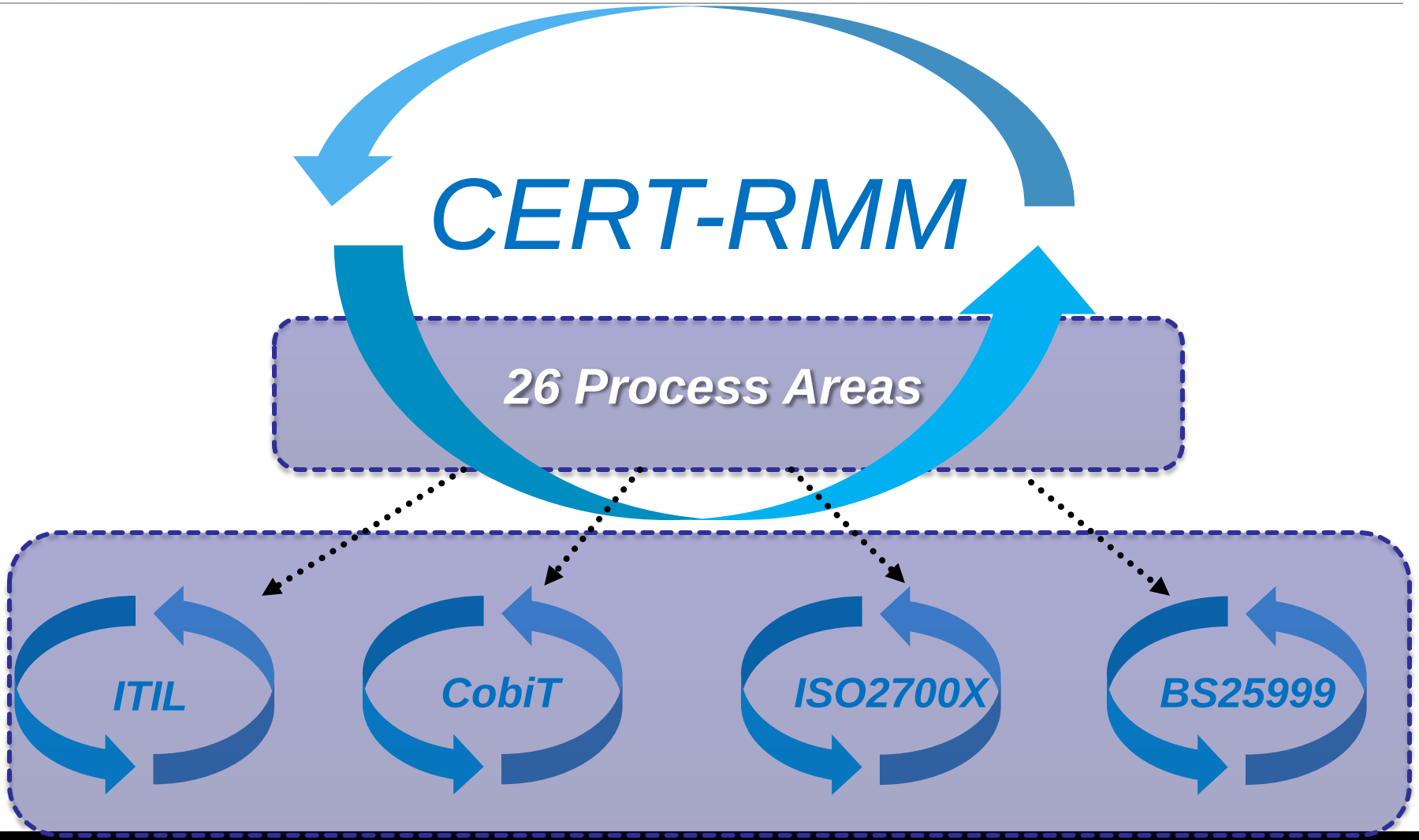
Overlap between CERT-RMM & CMMI process areas-1

CMMI Models Process Areas	Equivalent CERT-RMM Process Areas
CAM – Capacity and Availability Management *(CMMI-SVC only)*	**TM – Technology Management** Availability management is a central theme of CERT-RMM this includes PAs: RRD, RRM, EC, KIM, PM, TM
IRP – Incident Resolution and Prevention (CMMI-SVC only)	**IMC – Incident Management and Control**
MA – Measurement and Analysis	**MA – Measurement and Analysis is carried over intact from CMMI.**
OPD – Organizational Process Definition	**OPD – Organizational Process Definition is carried over from CMMI, but development life-cycle-related activities and examples are deemphasized or eliminated.**
OPF – Organizational Process Focus	**OPF – Organizational Process Focus is carried over intact from CMMI.**
OT – Organizational Training	**OTA – Organizational Training and Awareness** **OT is expanded to include awareness activities in OTA.**
REQM – Requirements Management	**RRM – Resilience Requirements Management** **Basic elements of REQM are included in RRM, but the focus is on managing the resilience requirements for assets and services, regardless of where they are in their development cycle.**
RD – Requirements Development	**RRD – Resilience Requirements Development** **Basic elements of RD are included in RRM, but practices differ substantially.**

Overlap between CERT-RMM & CMMI process areas-2 and Other Connections

CMMI Models Process Areas	Equivalent CERT-RMM Process Areas
RSKM – Risk Management	**RISK – Risk Management** Basic elements of RSKM are reflected in RRM, but the focus is on operational risk management activities and the enterprise risk management capabilities of the organization.
SAM – Supplier Agreement Management	**EXD – External Dependencies Management** In CERT-RMM, SAM is expanded to address all external dependencies, not only suppliers. EXD practices differ substantially.
SCON – Service Continuity *(CMMI-SVC only)*	**SC – Service Continuity** In CERT-RMM, SC is positioned as an operational risk management activity that addresses what is required to sustain assets and services balanced with preventive controls and strategies (as defined in CTRL – Controls Management).
TS – Technical Solution	**RTSE – Resilient Technical Solution Engineering** RTSE uses TS as the basis for conveying the consideration of resilience attributes as part of the technical solution.
Other Conncections: **Generic goals and practices**	The generic goals and practices have been adapted mostly intact from CMMI.
Other Connections: **Continuous representation**	CERT-RMM adopts the continuous representation concept from CMMI intact.

Example: CERT-RMM as an organizing principle



Current Approaches to Security Management

*Security by **compliance***

- *FISMA*
- *HIPAA*
- *PCI*

*Security by adoption of **best practices***

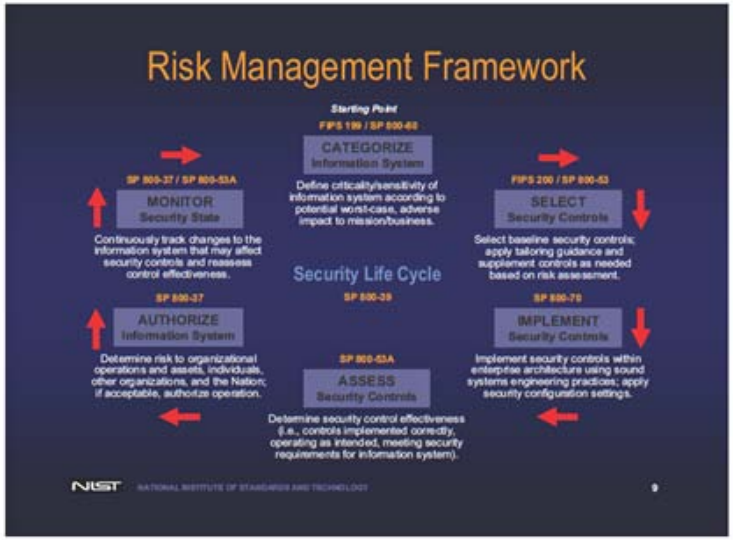
- *ISO 17799*
- *DISA STIGs*
- *Vendor guides*

Result:

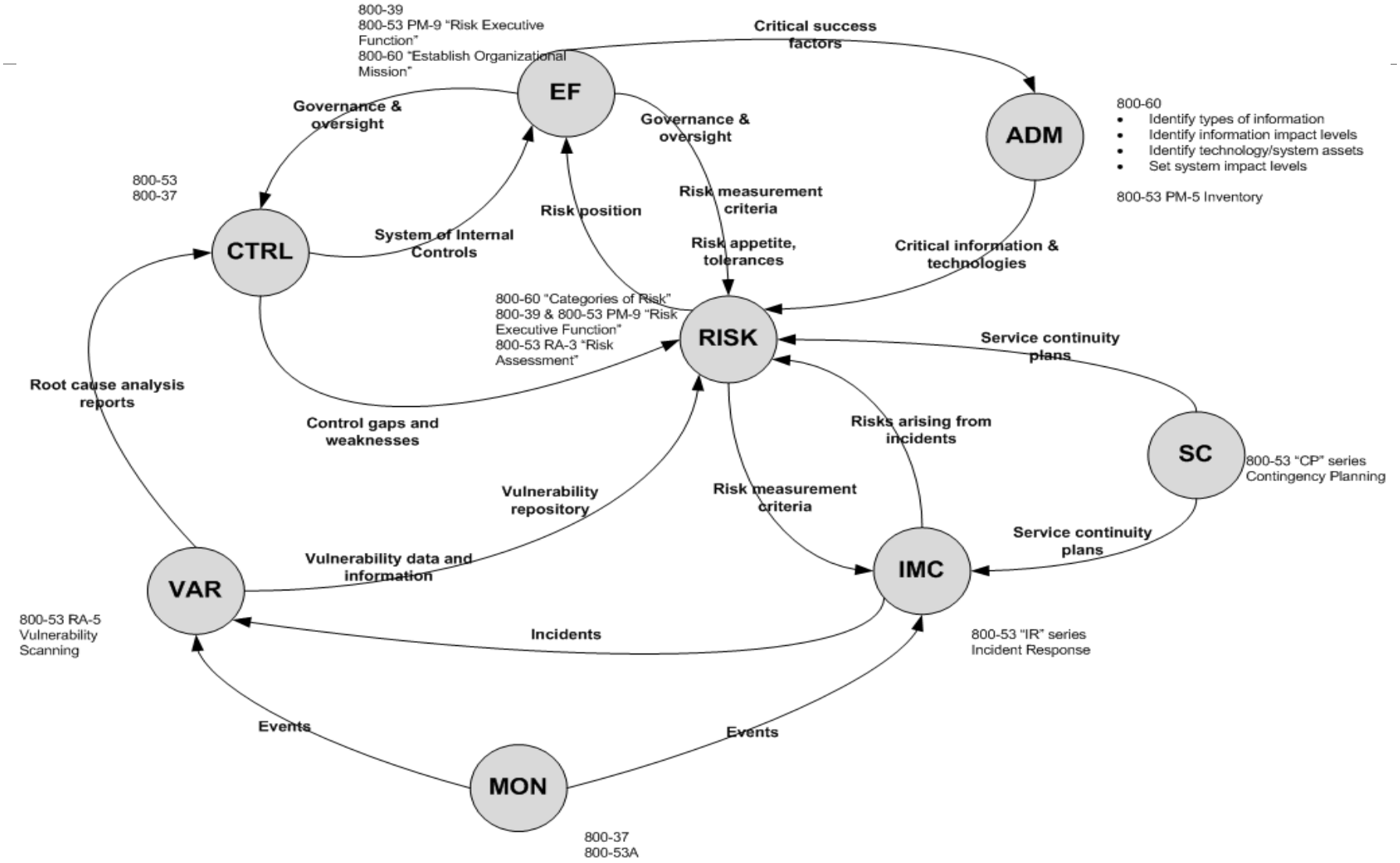
Uneven use of limited resources

Relationship to NIST Guidance

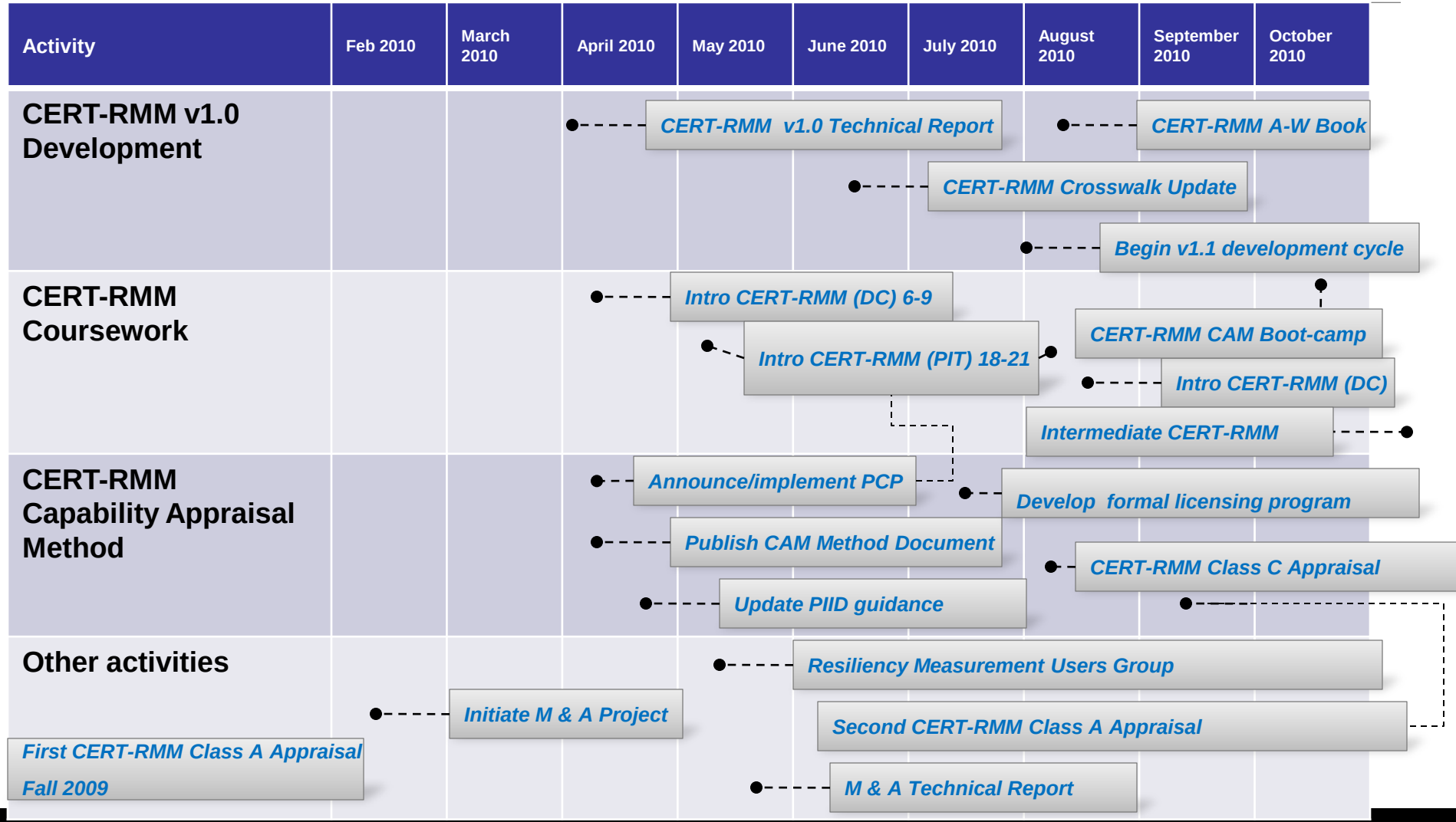
- NIST provides *guidance*
  - Risk Management Framework addresses controls management (800-37, 800-53, *et. al.)*
  - Risk Hierarchy forms the basis for an enterprise risk management program (800-39)
- RMM maps to a *risk ecosystem* to actualize and extend the NIST guidance



RMM Risk Ecosystem example



CERT-RMM Current Activities



Questions??

RMM Project Team and Contacts

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

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

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

Julia Allen
RMM Developer
jha@sei.cmu.edu

Richard E Barbour
RMM Appraisal Developer
reb@cert.org

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

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

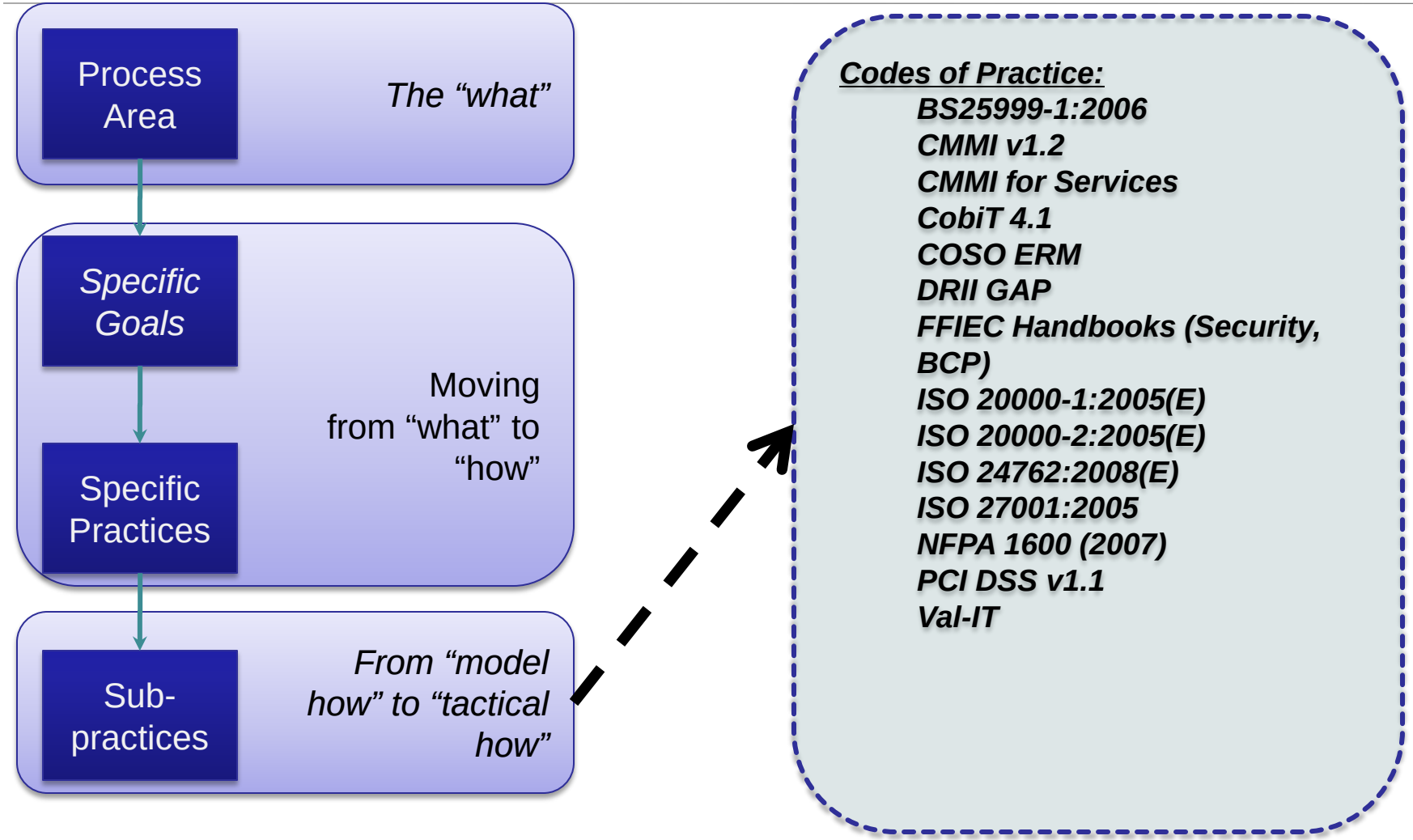
SEI Customer Relations
customer-relations@sei.cmu.edu
412-268-5800

www.cert.org/resiliency

Software Engineering Institute | Carnegie Mellon

Back-ups

CERT-RMM links to codes of practice

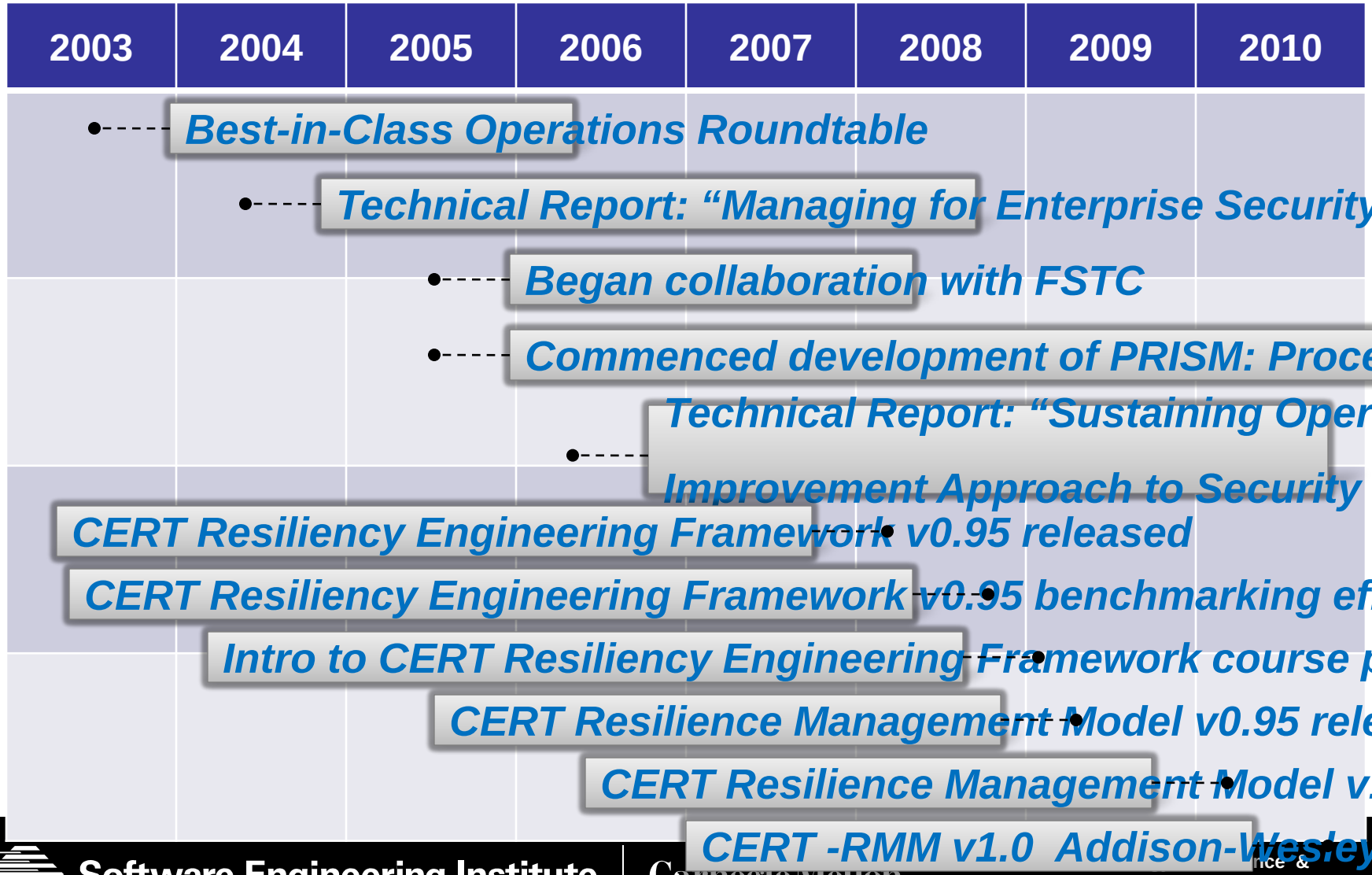


GAO-09-835T report says:

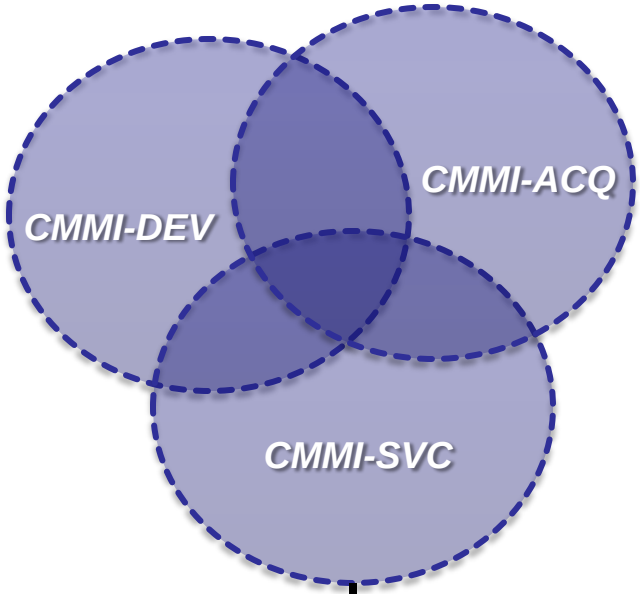
An underlying reason for the apparent dichotomy of increased compliance with security requirements and continued deficiencies in security controls is that the metrics defined by OMB and used for annual information security reporting do not generally measure the effectiveness of the controls and processes that are key to implementing an agency wide security program.

Results of our prior and ongoing work indicated that, for example, annual reporting did not always provide information on the quality or effectiveness of the processes agencies use to implement information security controls. Providing information on the effectiveness of controls and processes could further enhance the usefulness of the data for management and oversight of agency information security programs.

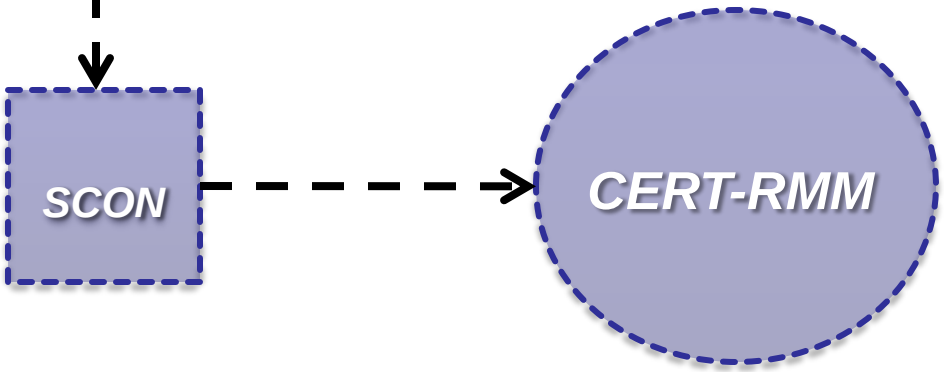
CERT-RMM timeline



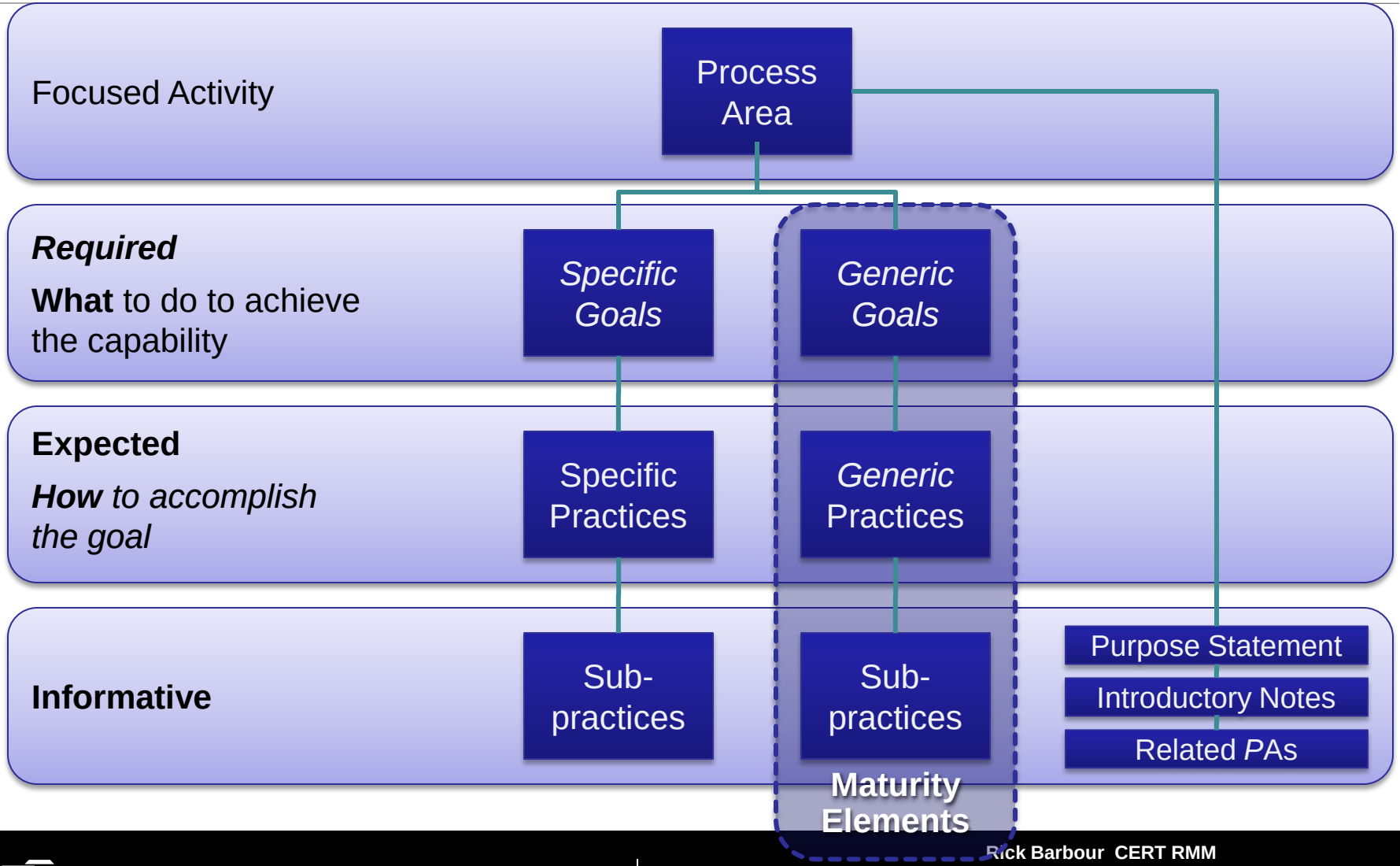
CERT-RMM and CMMI-SVC



- Expands SCON to resiliency perspective
- 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 process area structure



CERT-RMM Product Suite

Model artifacts available to begin an adoption process

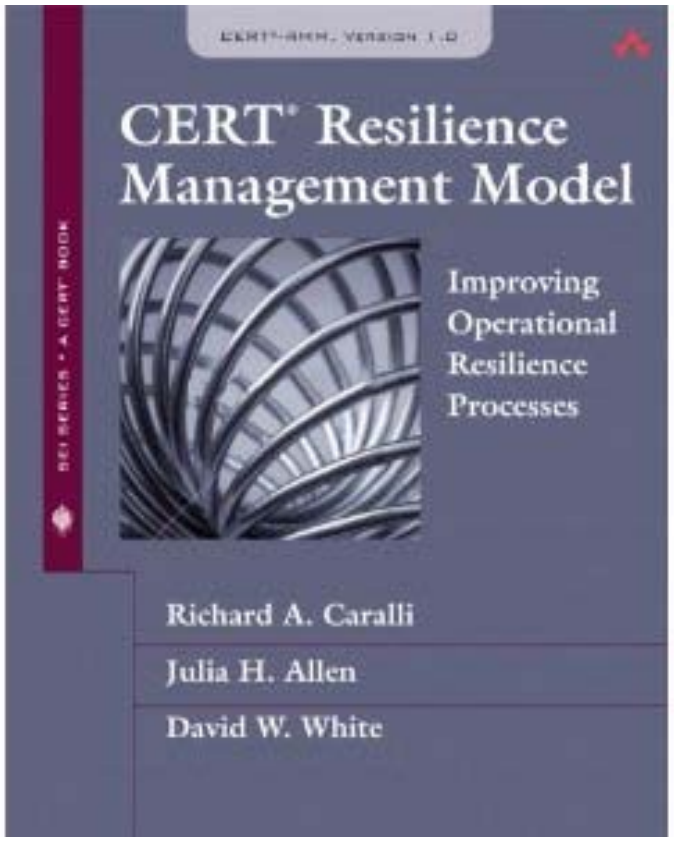
CERT-RMM product suite

Product	Status
CERT-RMM Model	Version 1.0 released; Technical Report released; individual process areas released @ www.cert.org/resilience
CERT-RMM Capability Appraisal Methodology	Version 1.0 to be released in method description document, August 2010
CERT-RMM Crosswalk	Version 0.95 published; Version 1.0 (expanded) to be published late Summer
Introductory courses	Introduction to CERT-RMM (4 days; offered 4 times/year in Pittsburgh and DC) Executive workshops and tutorials available on demand
Advanced courses	CERT-RMM Intermediate Course (in development for 2011) CERT-RMM CAM BootCamp (pilot scheduled for November 2010) CERT-RMM Role training (Coach, Navigator) CERT-RMM instructor training

CERT-RMM book publication

Scheduled for publication in November 2010 by Addison-Wesley

Includes full model (v1.0) plus adoption guidance and perspectives of real-world use of the model



Resilience measurement & analysis

- Area of research growing out of CERT-RMM development
- Focuses on the development of adequate measures to determine transformation of operational resilience management system
- Focuses on performance measurement—how well are we doing?
- Includes both qualitative and quantitative measurements
- Measurement users group (RMM MUG) forming—Fall 2010 opportunity to join a measurement cohort and share

One RMM Risk ecosystem

- Incident Management and Control (IMC)
- Vulnerability Analysis and Resolution (VAR)
- Compliance Mgmt. (COMP)
- Technology Management (TM)
- Knowledge and Information Management (KIM)
- Asset Definition and Management (ADM)
- Service Continuity (SC)
- Controls Management (CTRL)
- Enterprise Focus (EF)
- Monitoring (MON)

Alignment with NIST Risk Management Framework

RMM Risk Eco-System

Focused on operational *risk management* process

Provides the basis to actualize the NIST view of risk management (e.g. methods to examine conditions and consequences and link assets to services)

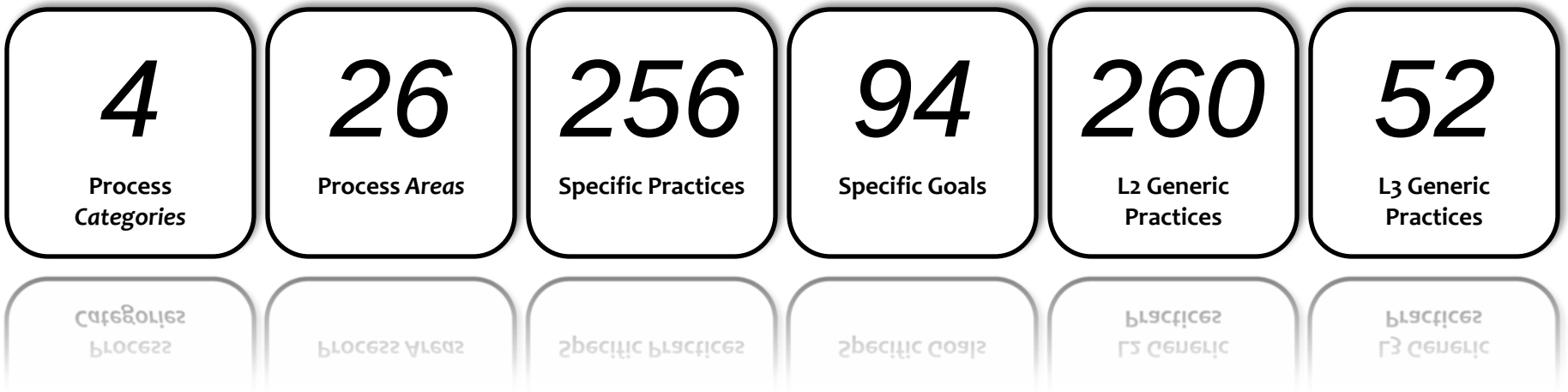
Provides the basis for a sustainable, repeatable, efficient and measurable risk management process

NIST RMF

Practical guidance for *risk assessment* of IT systems and application of controls

Provides foundation for the development of a threat management program based on control selection

CERT-RMM by the numbers



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 27001:2005
- NFPA 1600 (2007)
- PCI DSS v1.1

In progress or consideration:

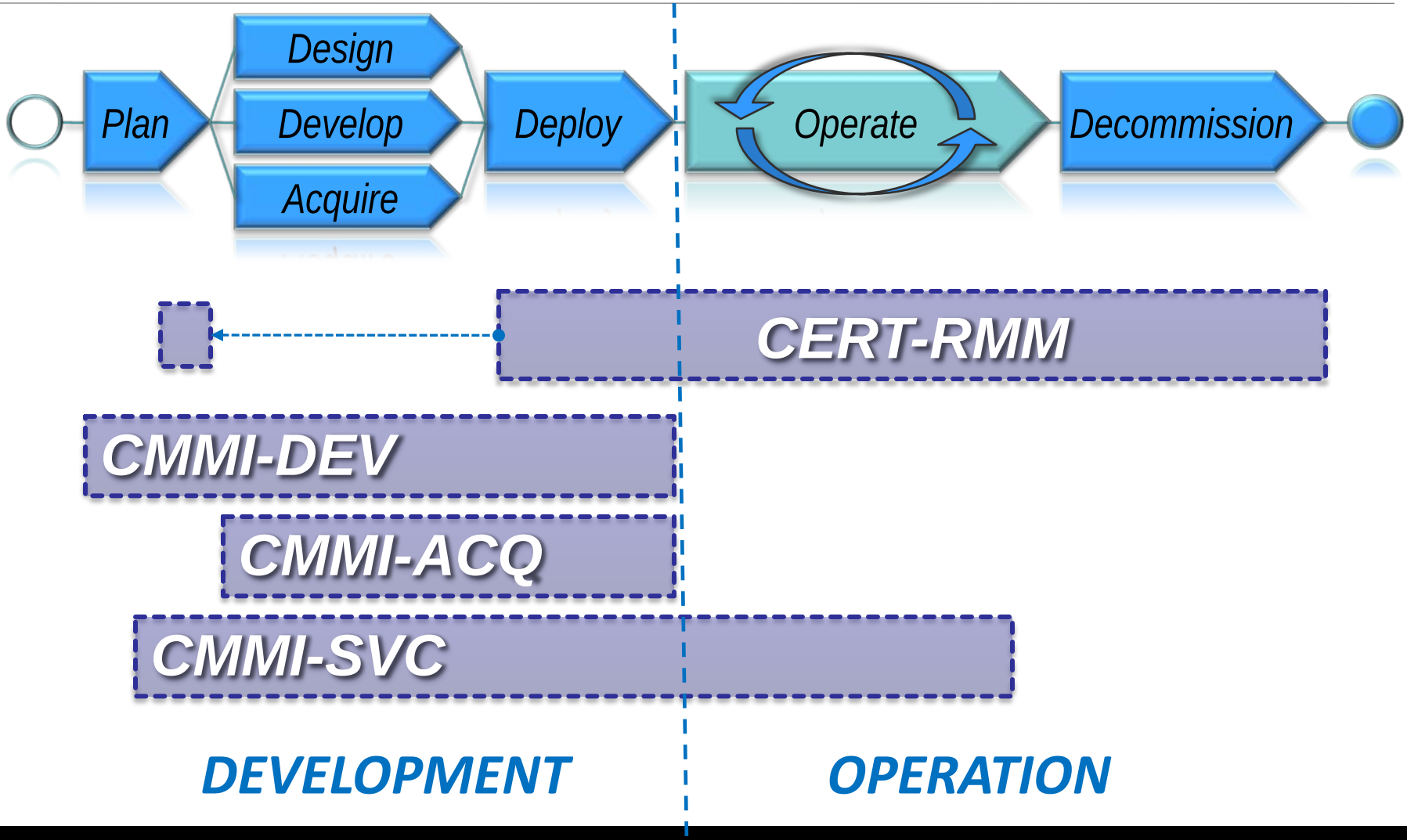
ISO SE7 Application Security Std

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

CERT-RMM position in lifecycle



Resiliency Project Members

AMD	IBM
Ameriprise	JPMorgan Chase
Bank of America	Key Bank
Carnegie Mellon	KPMG
Capital Group	MasterCard
Citicorp	Marshall and IIsley
Discover Financial	NY Federal Reserve Bank*
EMC	PNC Bank
DRII	US Bank
FSSCC R&D*	Wachovia

FSTC Financial Services Technology Consortium

CERT

RMM codifies best practices for security and business continuity from world leading organizations and numerous standards and codes

*Project Observer

Example: Asset Definition & Management

Goals	Practices
ADM:SG1 Establish Organizational Assets	ADM:SG1.SP1 Inventory Assets
	ADM:SG1.SP2 Establish a Common Understanding
	ADM:SG1.SP3 Establish Ownership and Custodianship
ADM:SG2 Establish Relationship Between Assets and Services	ADM:SG2.SP1 Associate Assets with Services
	ADM:SG2.SP2 Analyze Asset-Service Dependencies
ADM:SG3 Manage Assets	ADM:SG3.SP1 Identify Change Criteria
	ADM:SG3.SP2 Maintain Changes to Assets and Inventory

Institutionalizing *Asset Definition & Management*

Goals	Practices
ADM:SG1 Establish Organizational Assets	ADM:SG1.SP1 Inventory Assets
	ADM:SG1.SP2 Establish a Common Understanding
	ADM:SG1.SP3 Establish Ownership and Custodianship
ADM:SG2 Establish Relationship Between Assets and Services	ADM:SG2.SP1 Associate Assets with Services
	ADM:SG2.SP2 Analyze Asset-Service Dependencies
ADM:SG3 Manage Assets	ADM:SG3.SP1 Identify Change Criteria
	ADM:SG3.SP2 Maintain Changes to Assets and Inventory

A **managed** process is:

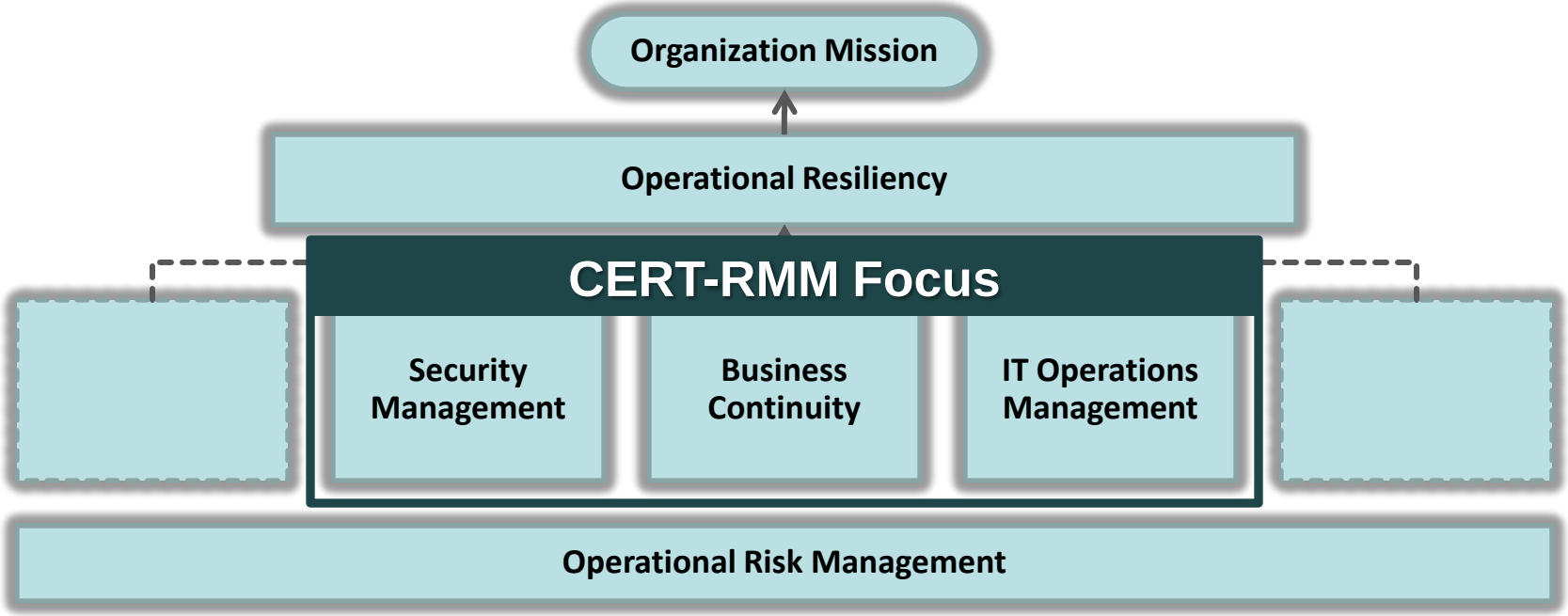
- Governed
- Executed according to policy
- Employs skilled people
- Involves relevant stakeholders
- Monitored, controlled, and reviewed
- Evaluated for adherence to the organization's process description
- Regularly reviewed with senior management

Practice example: *ADM.SG1.SP1-Inventory Assets*

To institutionalize the performance of the "Inventory Assets" practice, you must commit to and perform these supporting practices:

Institutionalizing Factor	Institutionalizing Practice
Governed	There is a policy requiring periodic asset inventory activities; the activity has oversight and corrective actions are taken when necessary
Employs skilled people	Staff involved in the practice have the appropriate skill levels and training
Involves stakeholders	Asset owners and custodians are involved; all involved in protecting and sustaining the asset are involved
Monitored and controlled	The process is measured to determine effectiveness. Examples: % of assets inventoried; # of changes to inventory in a given period
Evaluate adherence	The process as performed is verified to be aligned with the process definition
Review with senior management	Keep management informed on the results of the process and identify and resolve issues

CERT-RMM principle of convergence



Operational resilience is directly affected by convergence

Organizational mission is directly affected by operational resilience

Positioning CERT-RMM in CMMI