Resilient Service: CMMI –SVC and CERT-RMM

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

November 2011

Eileen Forrester, Richard Caralli

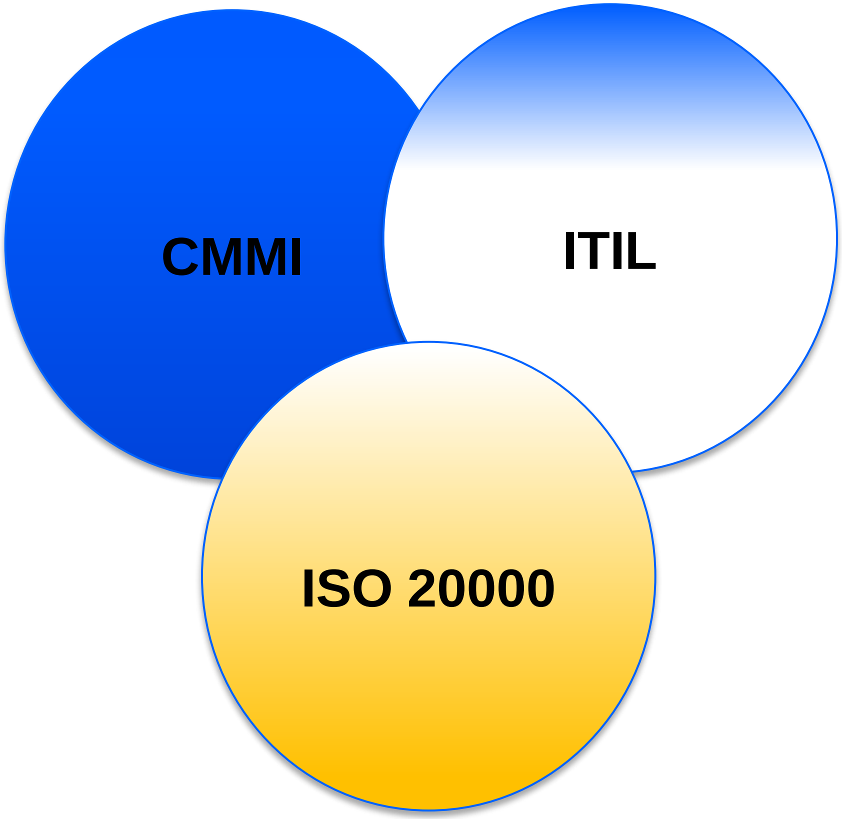
What we will cover

- An alternate way to get some security coverage
- What is resilient service
- CMMI-SVC and RMM
- Quality and mission assurance
- An example resilient service using both models

Assembling a multi-model approach to improving service quality and ensuring service resilience in complex risk environments

AIM
RMM
SIX SIGMA
ISO
TSP
COBIT
ITIL
CMMI-SVC

Improving Service Management



Why Should We Fill the Gap?

Completeness of Improvement Journey

- Organizations have business problems to solve that cross model boundaries
- Framing these issues in a common language helps

Appraisal or Audit or Compliance Need

- Organizations with multiple accreditations are faced with frequent internal audit and appraisal issues
- One common framework cuts appraisal and audit costs & minimizes disruption to busy front line workers

Model Completeness

- Security issues are not "additional" to service delivery they are integral to it

How To Fill The Gap?

RMM?

- Lots of great material
- High specification of how to solve security questions
- Probably interpreted in some people's minds as "An Extra Model to adopt!"

Services PA

- Services security content needs steward approval

CMMI-SVC "Pseudo PA" Material

- Quick
- Seed for further development
- Small scale addition to existing model

Developing a “Bolt on” for CMMI

Requirements

- Needs to work with other CMMI process areas
- Needs to have fit CMMI architecture
  - Required Components
  - Expected Components
  - Informative Material
- Generic Practices
- Specific Material

GP Relationship - Conclusions

ISO 27001 clauses are short statements of requirements

- Not much detail
- No “informative material” – example work products, etc.

ISO 27001 – Is less explicit on Stakeholder Management

Using CMMI GPs would

- Further help embed good practice
- Build upon existing material

ISO 27001 – Establishing ISMS

Clause 4.2.1 - Establish the Information Security Management System

- Scope the security system
- Define an approach to identifying and evaluating security threats
- Define how to deal with them
- Obtain management approval for the plans and mechanisms defined

ISO 27001 – Put the ISMS in Place

Clause 4.2.2 - Implement and Operate the Information Security Management System

- Instigate a plan to operate the security system
- Manage the level of threat.

Clause 4.2.3 - Monitor and Review the ISMS

- Use ISMS mechanisms to monitor threats
- Take action to address threats

Clause 4.2.4 - Maintain and Improve the ISMS

- Measuring and monitor the system
- Implement corrections or improvements

Security Pseudo PA – Basic Structure

Examination of ISO 27001 provided a nice suggestion of initial content

- Establish and Maintain a Security Management System
- Use the Agreed Security Management System to Provide Required Security
- Note we dropped “information” in our version

Under these two strands we can construct statements that look and feel like practice statements

- Ideal for appraisal purposes
- Very valuable for improvement teams constructing an improvement plan
- One language style, one plan, potentially multiple models engaged

Pseudo PA:
Security Management (SM)

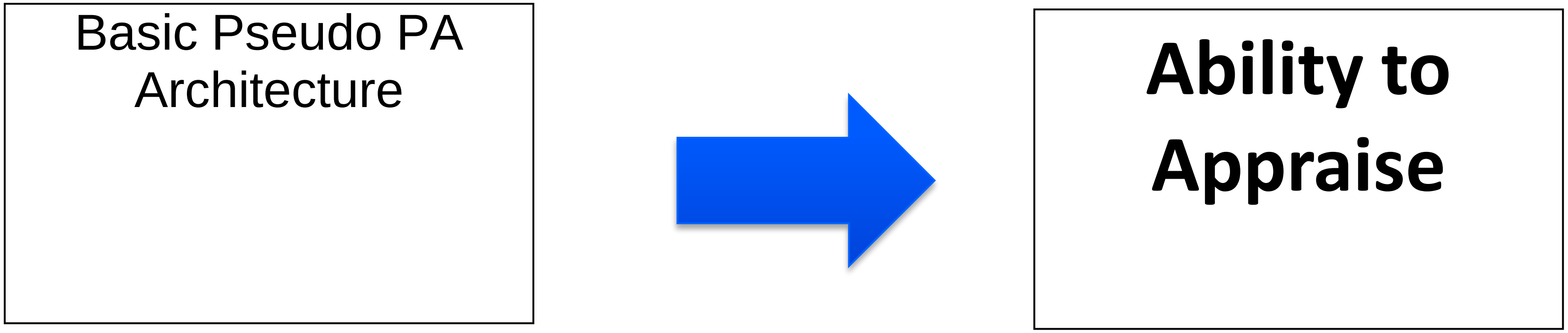
ESG1 – Establish a Security Management System

- ESP1.1 Establish Security Objectives
- ESP1.2 Establish an Approach to Threat Assessment
- ESP1.3 Identify Security Threats
- ESP1.4 Evaluate and Prioritize Security Threats
- ESP1.5 Establish a Security Management Plan
- ESP1.6 Obtain Commitment to the Security Management Plan

ESG2 – Provide Security

- ESP2.1 Operate the Security Management System
- ESP2.2 Monitor the Security Management System

Framework For Building Upon



Basic Pseudo PA Architecture

Ability to Appraise

But ….

CMMI is used for more than appraisals, what about the implementation and improvement

Informative Material

Informative Material provides:

- Subpractices
- Notes
- Examples
- Elaborations
- Example Work Products
- Etc.

All these help the implementation of good practice

This PA is quite general, so RMM is also a source for more detail and rigor.

Example New Informative Material

ESP1.2 Establish an Approach to Threat Assessment

Establish and maintain an approach to assessing vulnerabilities and threats to essential assets.

Subpractices

1. Select methods for assessing security threats
2. Define criteria for evaluating and quantifying security threats.
3. Describe responsibility and resources for evaluating vulnerabilities and threats.

Next Moves

Pseudo PA has been tested on a number of appraisals

Challenge to develop more “PA” like substructure

- Practices
- Subpractices
- Example work products
- GP Elaborations

We have made a start–but now would like to engage a wider audience to take the discussion forward

Community Feedback and Input

Should this work be taken further?

Is the scope useful for improvement?

What could be done next to make it more credible?

We would like your comments.

- cmmi-comments@sei.cmu.edu.

Some Useful Links

CMMI for Services Model

http://www.sei.cmu.edu/cmmi/tools/svc/index.cfm

CMMI for Services and Security Whitepaper

http://www.sei.cmu.edu/cmmi/tools/svc/upload/Security-and-CMMI-SVC.pdf

CMMI for Services Book

http://www.amazon.com/CMMI-Services-Guidelines-Superior-Engineering/dp/0321711521/ref=sr_1_1?ie=UTF8&qid=1304415568&sr=8-1

Summary on the Pseudo PA

ISO20000, ITIL, & CMMI all work very well together

CMMI misses one component in common with the other approaches: security

ISO 27001 provided a starting point for developing a “pseudo” process area: SM

We are seeking community input to develop this pseudo process area further

How Resilient Am I? - 1

When asked:

- How resilient am I?
- Am I resilient enough?
- How resilient do I need to be?

what does this mean?

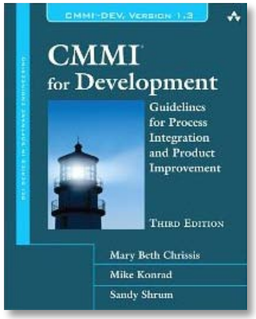
How Resilient Am I? - 2

- Do I need to worry about operational resilience?
- If services are disrupted, will it make the news? Will I end up in court? in jail? Will I be able to stay in business?
- Do I meet compliance requirements?
- How resilient am I compared to my competition?
- Do I need to spend more $$ on resilience? If so, on what?
- What am I getting for the $$ I've already spent?

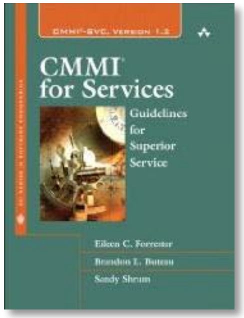
What is CMMI?

The Capability Maturity Model Integration (CMMI)

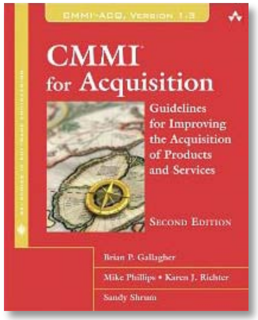
- is a framework for management practices
- provides organizations with the essential elements of effective processes that improve performance
- can be used as a benchmark, but is about quality improvement



CMMI for Development (CMMI-DEV)



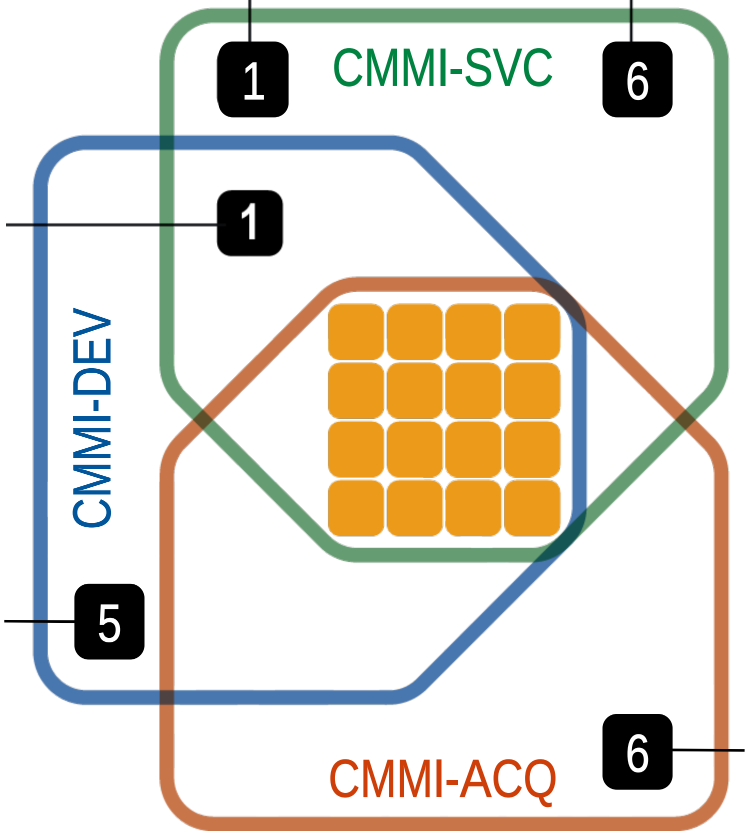
CMMI for Services (CMMI-SVC)


CMMI-ACQ, Version 1.3
CMMI for Acquisition
Guidelines for Improving the Acquisition of Products and Services
Second Edition
Brian P. Gallagher
Mike Phillips • Karen J. Richter
Sandy Shrum

CMMI for Acquisition (CMMI-ACQ)

The CMMI Product Suite is a set of CMMI-related products that includes CMMI models, appraisal method, and CMMI training courses.

Relationships Among CMMI Models



Service "addition" PA (SSD)

Service-specific PAs

Shared PA (SAM)

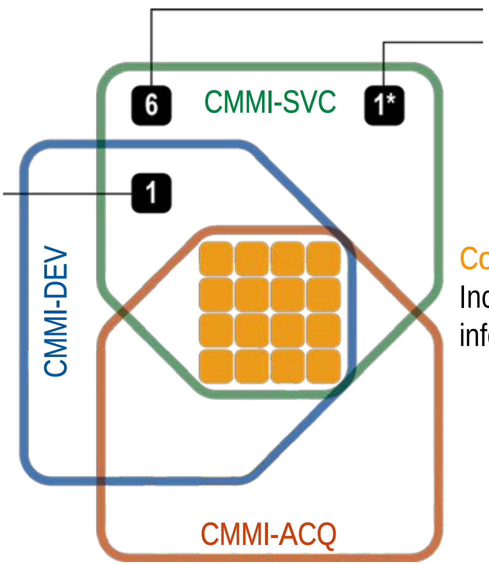
Core PAs

Include model-specific informative material

Development-specific PAs

Acquisition-specific PAs

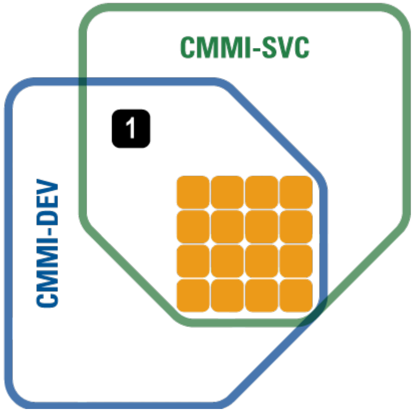
A Look at CMMI-SVC



Services-specific PAs
*CMMI-SVC addition

Shared PA
(SAM)

Core PAs
Include service-specific informative material



CAM	Capacity and Availability Management
IRP	Incident Resolution & Prevention
SCON	Service Continuity
SD	Service Delivery
STSM	Strategic Service Management
SST	Service System Transition
SSD	Service System Development

Define, and Establish, and Deliver Services
SD REQM WP SSD

Monitor and Control Service and Work Products
CAM WMC CM

Ensure Service Mission Success
IRP RSKM SCON SST

Make Work Explicit and Measurable
MA OPP QWM CAR OPM

Manage Decisions, Suppliers, and Standard Services
SAM DAR STSM

Create a Culture to Sustain Service Excellence
PPQA OPD IWM OT OPF

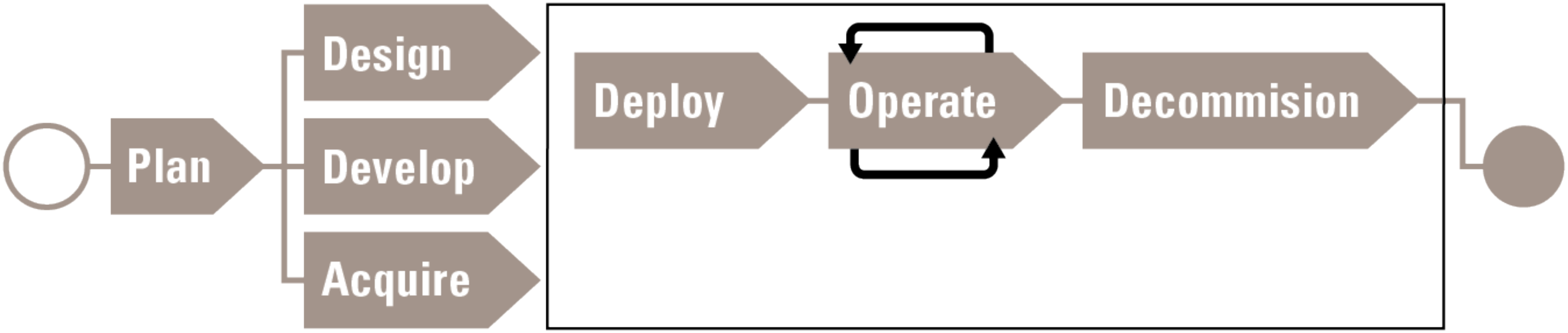
What is CERT®-RMM?

CERT-RMM is a capability 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**

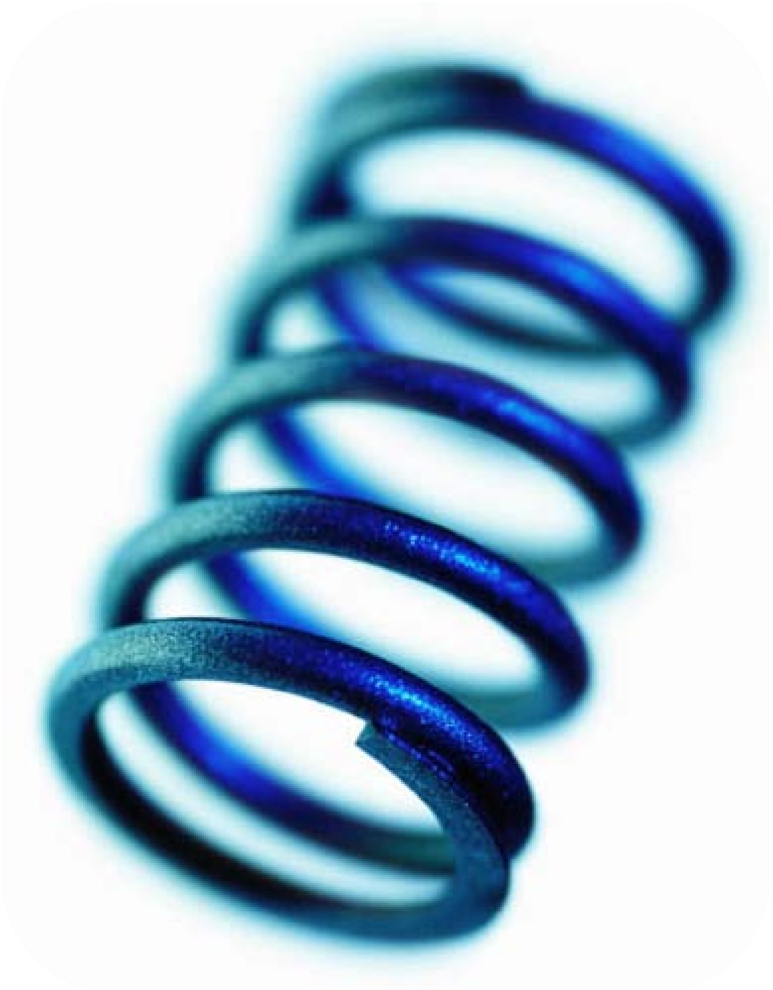
CERT-RMM in the life-cycle

Operational resilience management focuses on the deploy, operate, and decommission phases, but reaches back to development phase of lifecycle to ensure consideration of security and continuity issues prior to placing assets in production.



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* that can *continue to carry out its mission* after *disruption* that *does not exceed* its *operational* limit

[CERT-RMM]

Services in CERT-RMM

The resilience of **high-value services** ensures the resilience of the **mission.**

Service resilience is a factor of **asset resilience**—if an asset is disrupted or fails, the service may suffer.

Service resilience is the object of CERT-RMM processes.

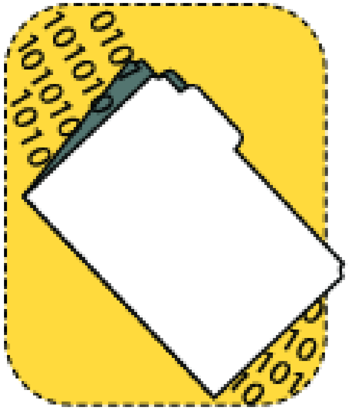
Assets

Something of value to the organization

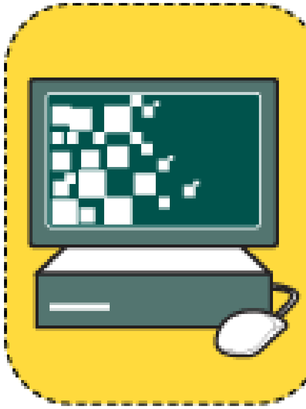
Used by business processes and services

CERT-RMM focuses on four types:

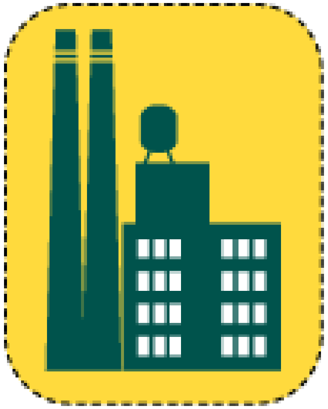
People



Information

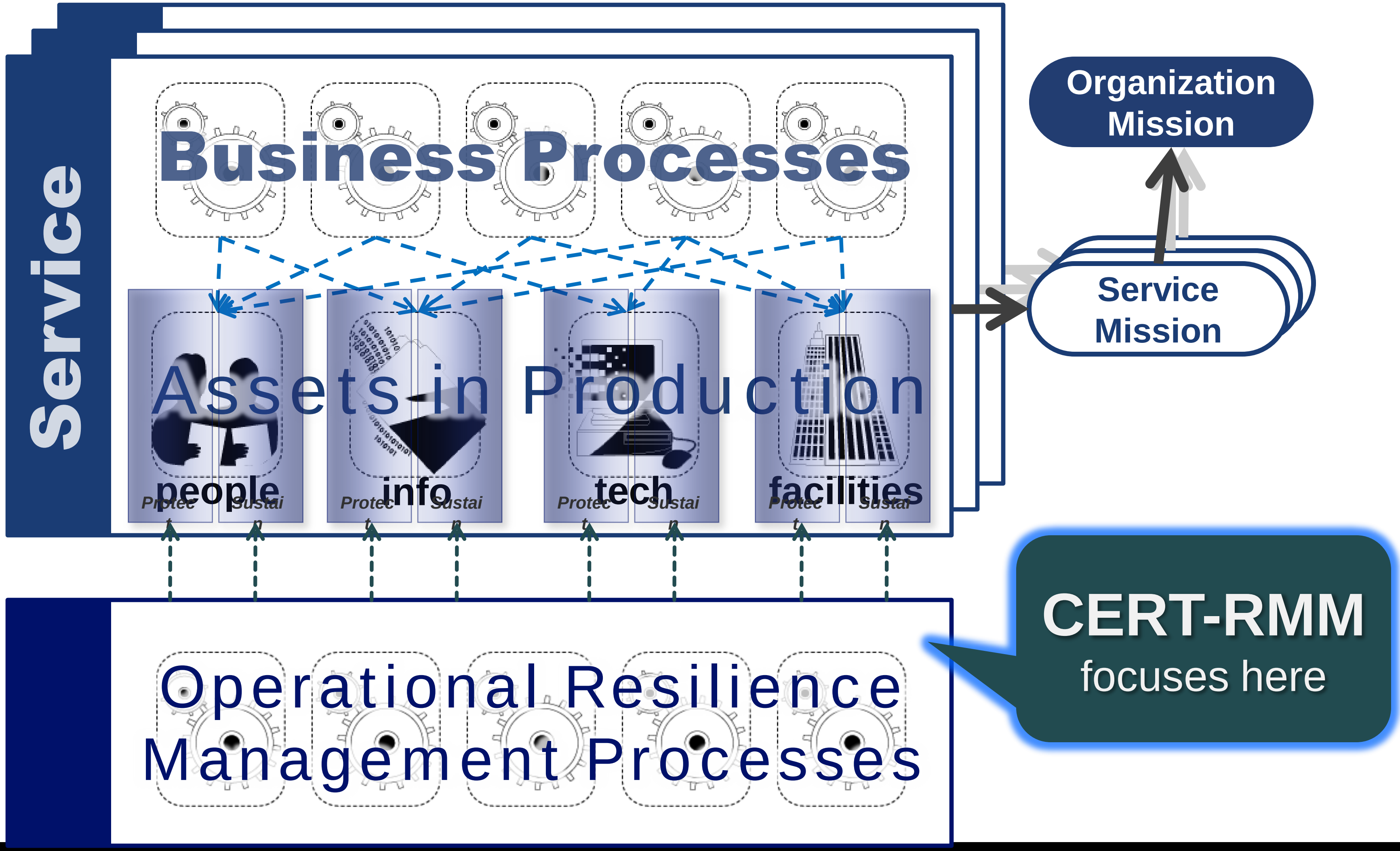


Technology



Facilities

Organizational Context



Service

Business Processes

Assets in Production

people

Protect Sustain

info

Protect Sustain

tech

Protect Sustain

facilities

Protect Sustain

Operational Resilience Management Processes

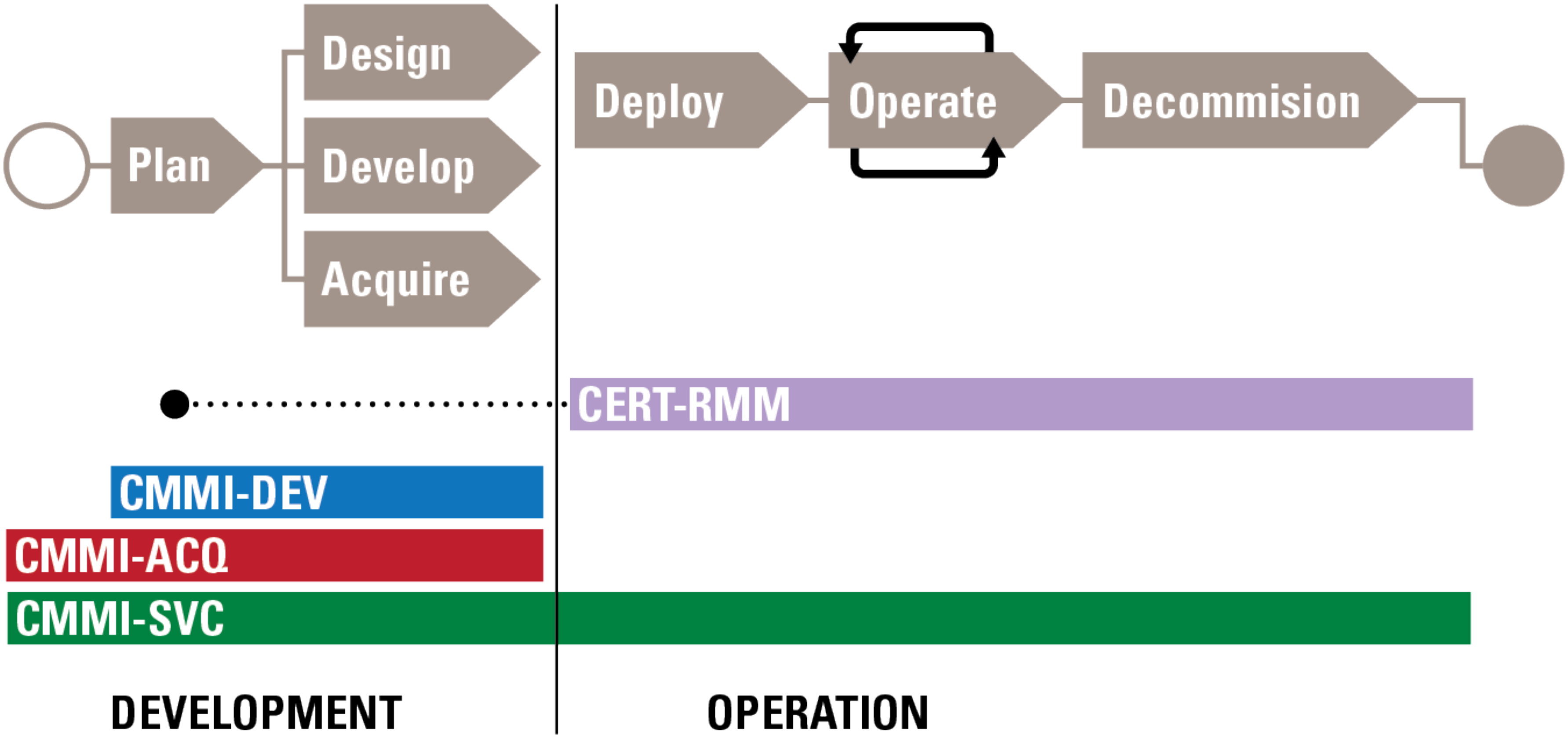
Organization Mission

Service Mission

CERT-RMM

focuses here

CERT-RMM & CMMI in the life cycle



CERT-RMM architectural elements

CERT-RMM uses proven architectural elements of CMMI and applies them in an operational context.

- 26 process areas
- Arranged in a continuous representation
- Goals, practices, sub-practices, and work products that *specifically* define each process area
- Goals, practices, and sub-practices that *generically* define increasing levels of capability
- Implementation and adoption examples
- An appraisal methodology to determine capability levels

CERT-RMM at a glance

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

26 Process Areas in 4 categories

Enterprise management

Seven process areas that support the resilience management process

Governance, Risk, & Compliance

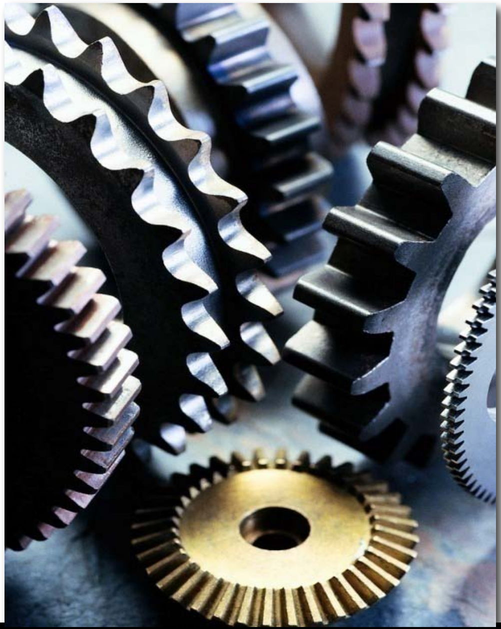
COMP EF RISK

Supporting Resilience

COMM FRM HRM OTA

Engineering

Six process areas for establishing resilience for organizational assets, business processes, and services



Asset Management

ADM

Requirements Management

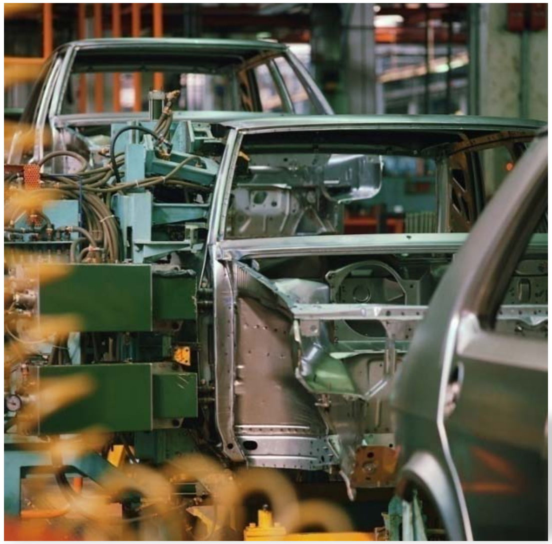
RRD RRM

Establishing and Managing Resilience

CTRL RTSE SC

Operations management

Nine process areas for managing the operational aspects of resilience



Asset Resilience Management

EC KIM PM TM

Threat, Incident, & Access Management

AM ID IMC VAR

Supplier Management

EXD

Process management process areas

Four process areas for defining, planning, deploying, implementing, monitoring, controlling, appraising, measuring, and improving operational resilience management processes

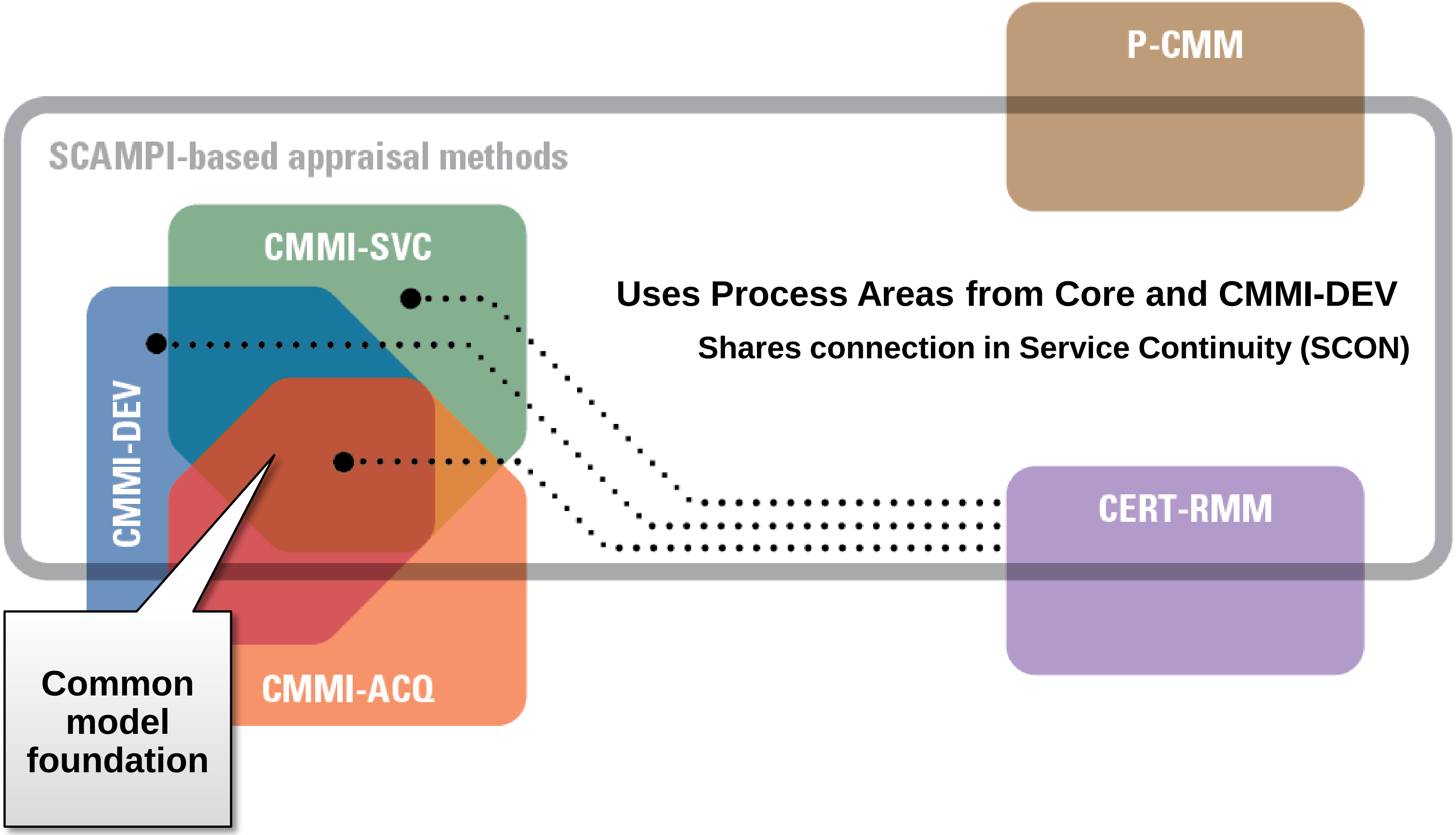
Data Collection & Logging

MON

Process Management

MA OPD OPF

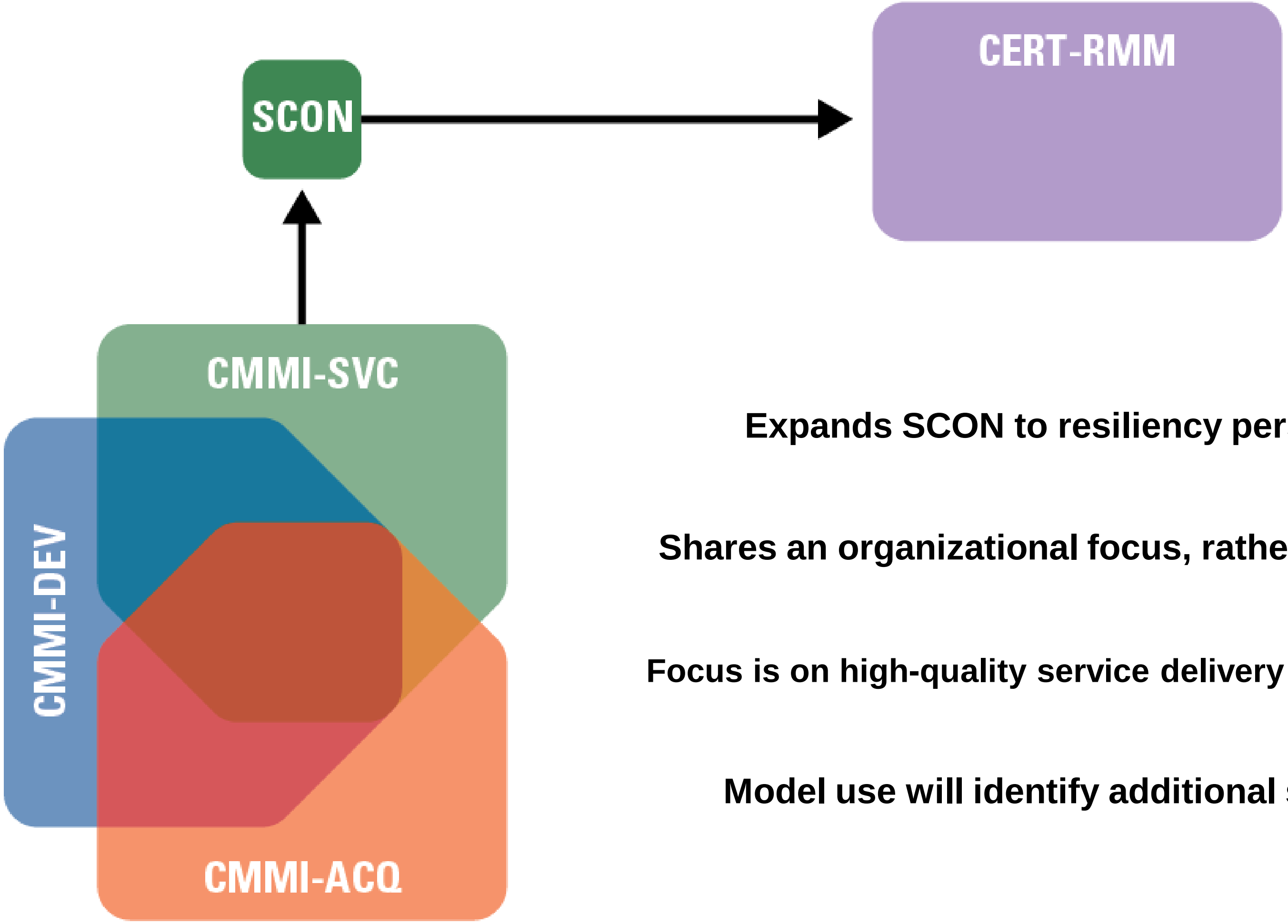
Positioning CERT-RMM with CMMI



Uses Process Areas from Core and CMMI-DEV

Shares connection in Service Continuity (SCON)

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

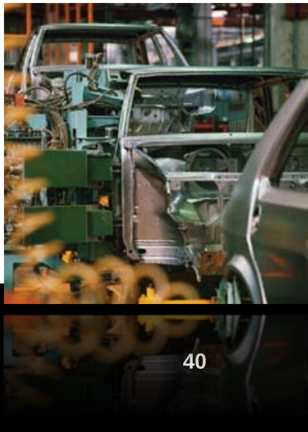
A service example: US auto insurance

Olive Vehicle Insurance (OVIG) provides car and light truck insurance.

Customer services include providing quotes, issuing policies, billing and processing premiums, processing claims, providing legal services, and providing vehicle repair.

They pride themselves on being easy to reach and quick to act when the customer needs them. They are facing an increasingly demanding regulatory environment in the US.

What does it mean for these services to be resilient? What assets must be resilient? What practices in RMM go beyond RSKM, IRP, and SCON?



CMMI-SVC PAs that ensure mission success

Incident Resolution and Prevention (IRP):

- handling what goes wrong—and preventing it from going wrong ahead of time if you can

Risk Management (RSKM):

- supporting the success of your service mission by anticipating problems and how you will handle them—before they occur

Service Continuity Management (SCON):

- being ready to recover from a disaster and get back to delivering your service

Service System Transition (SST):

- getting new systems in place, changing existing systems, and retiring obsolete systems, all while making sure nothing goes terribly wrong with service

CMMI-SVC PAs taken further with RMM PAs

Incident Resolution and Prevention (IRP):

- IMC is obvious, but also VAR in RMM goes further than goal 3 in IRP to actively watch and resolve vulnerabilities before they become incidents that disrupt insurance services

Risk Management (RSKM):

- KIM practices can be used to apply controls for confidentiality, integrity, and availability to critical data, such as customer information
- CTRL practices go further to applying controls to service processes such as paying claims, so that, for example, no claim is paid twice and that claim data is kept confidential and not accidentally modified

Service Continuity Management (SCON):

- SC in RMM explodes the goals and practices found in SCON with considerably more detail; for example, a data-intensive service like insurance can find more advice on managing effects on vital records; in addition, SC makes clear the distinctions among continuity, recovery, and restoration of service

Also consider:

EXD, which goes further than SAM to further resilience, more info on external dependencies and service agreements

MON, which goes beyond MA in SVC to have “feelers” out for data so that the organization knows how their data stands relative to threats and vulnerabilities

Summary

GPs and Pseudo PA approach allows you to selectively borrow from additional models, even during appraisal.

RMM and CMMI-SVC combination:

- The goal of CMMI-SVC is equip organizations to improve processes and ensure high-quality service management and delivery at an affordable cost.
- The goal of CERT-RMM is to improve processes to ensure that essential organizational services meet their mission consistently in the face of shifting operational risk.
- They share common content, similar product suites to support use, and provide different detail and specificity that you can choose from to meet your precise needs.
- These two models are being combined in appraisal and implementation.
- In short, CMMI-SVC and CERT-RMM are synergistic and amenable to a continuous approach based on your business needs for resilient service.

CERT-RMM contacts

Rich Caralli

RMM Architect and Lead Developer
rcaralli@cert.org

Lisa Young

RMM Appraisal Lead and Developer
lry@cert.org

Richard Lynch

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 and Developer
dwhite@cert.org

Julia Allen

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

SEI Customer Relations

customer-relations@sei.cmu.edu
412-268-5800

http://www.cert.org/resilience/

Contact information

Eileen Forrester
Manager, CMMI for Services
SEPM
Telephone: +1 412-268-6377
Email: ecf@sei.cmu.edu

Web
www.sei.cmu.edu/cmmi
www.sei.cmu.edu

U.S. Mail
Software Engineering Institute
Customer Relations
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
USA

Email:	info@sei.cmu.edu
Telephone:	+1 412-268-5800
SEI Phone:	+1 412-268-5800
SEI Fax:	+1 412-268-6257

Backup slides as needed

Imperatives for building CERT-RMM

Tech reliance

Global economy

Open boundaries

Complexity

Cultural shifts

Increasingly complex operational environments; traditional approaches failing

Silo nature of operational risk activities; a lack of convergence

Lack of common language or taxonomy

Overreliance on technical approaches

Lack of means to measure organizational capability

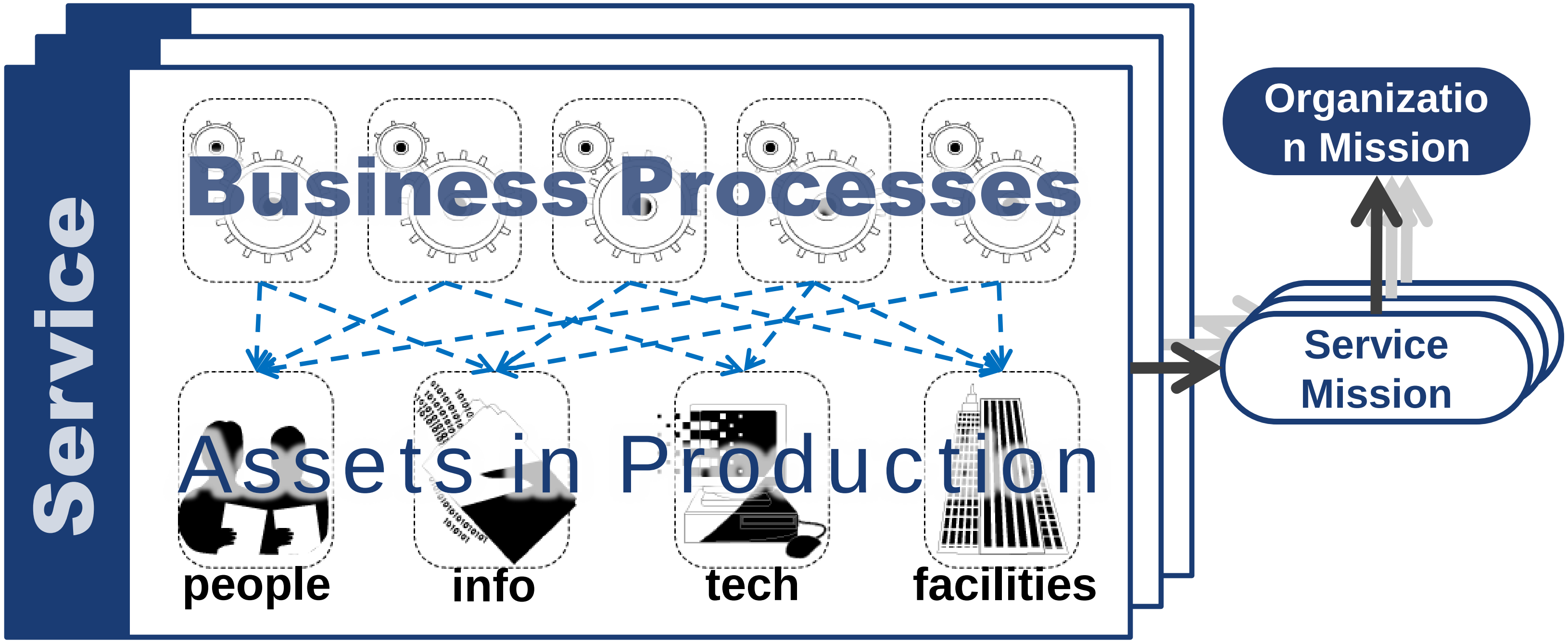
Inability to confidently predict outcomes, behaviors, and performance under times of stress

How Resilient Am I? - 3

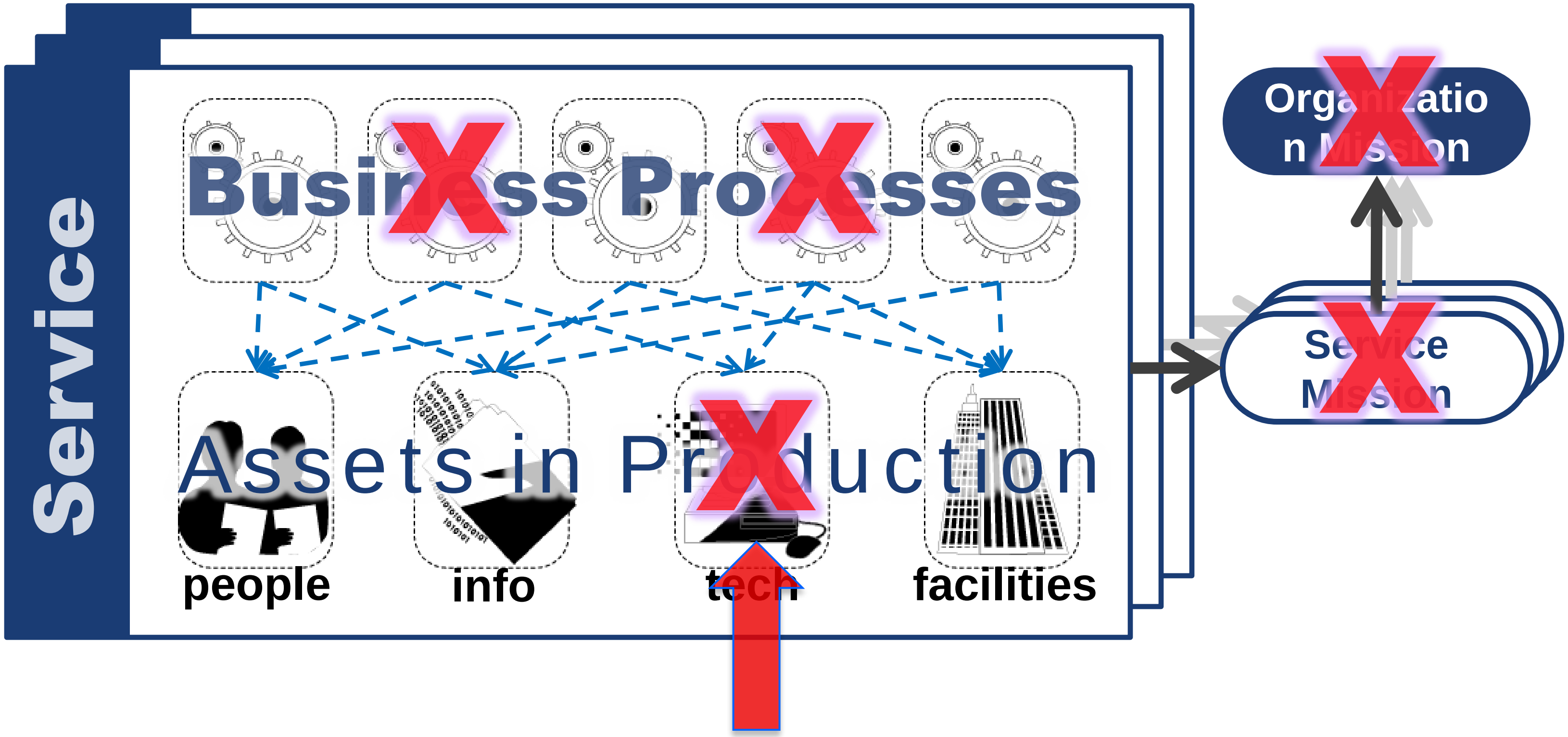
What should I be measuring to determine if I am meeting my performance objectives for resilience?

What is the business value of being more resilient?

Organizational context



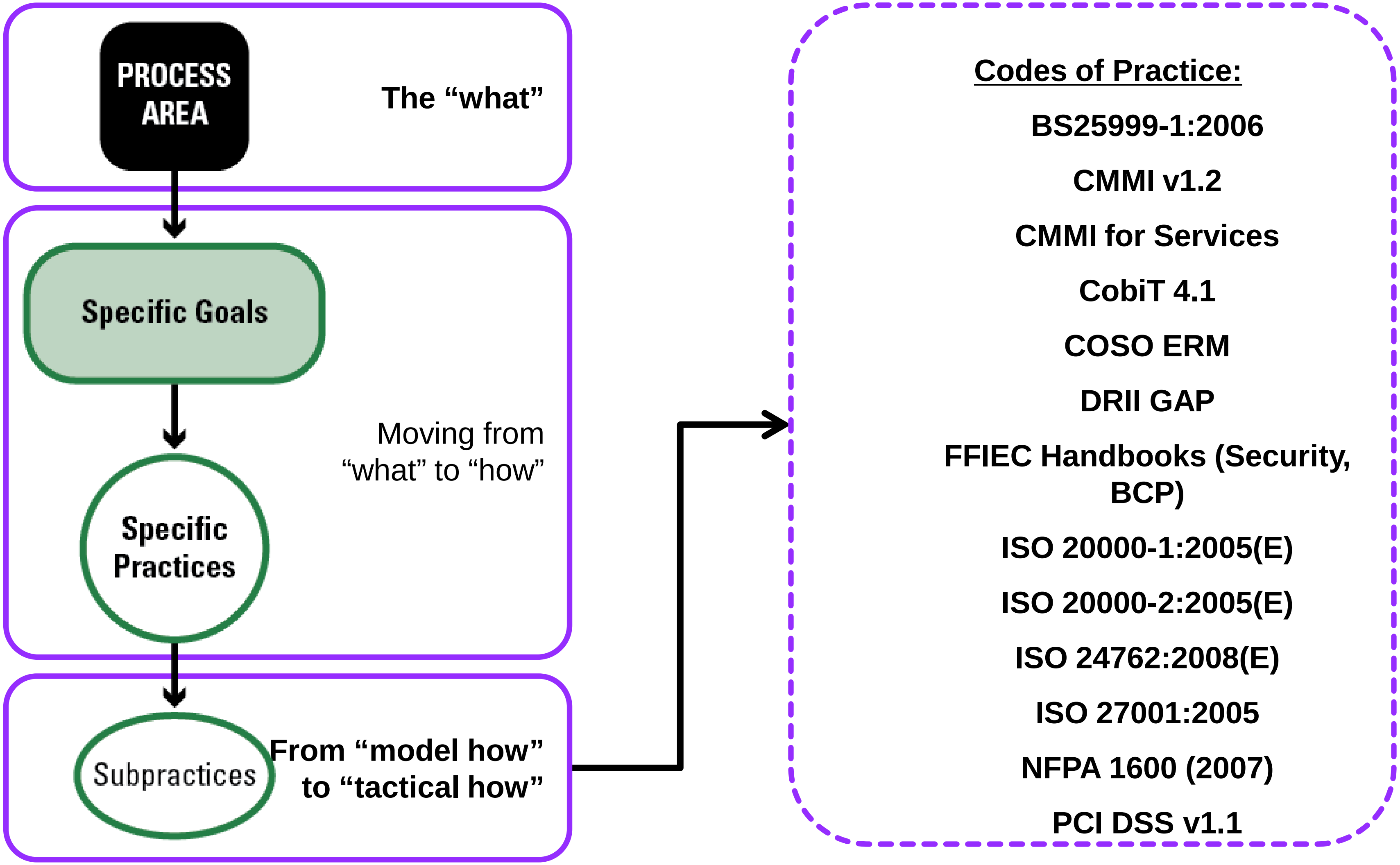
Organizational context - disruption



Operational risk can disrupt an asset

And lead to organizational disruption

CERT-RMM links to codes of practice



Codes of Practice:

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

How Resilient Am I? - 1

When asked:

- How resilient am I?
- Am I resilient enough?
- How resilient do I need to be?

what does this mean?

How Resilient Am I? - 2

- Do I need to worry about operational resilience?
- If services are disrupted, will it make the news? Will I end up in court? in jail? Will I be able to stay in business?
- Do I meet compliance requirements?
- How resilient am I compared to my competition?
- Do I need to spend more $$ on resilience? If so, on what?
- What am I getting for the $$ I've already spent?