Moving Your Security, Business Continuity, and IT Activities to the Next Level Using the CERT® Resiliency Management Model

CMMI® Technology Conference and User Group

19 November 2009

Gibbie Hart

Rick Barbour

Briefing Outline

Introduction

Building Blocks of Resiliency Engineering

CERT® RMM Overview

RMM Current & Planned Activities

Summary

Questions

Resiliency 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.

Organizational and operational challenges

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!

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
- IT operations and service delivery management

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

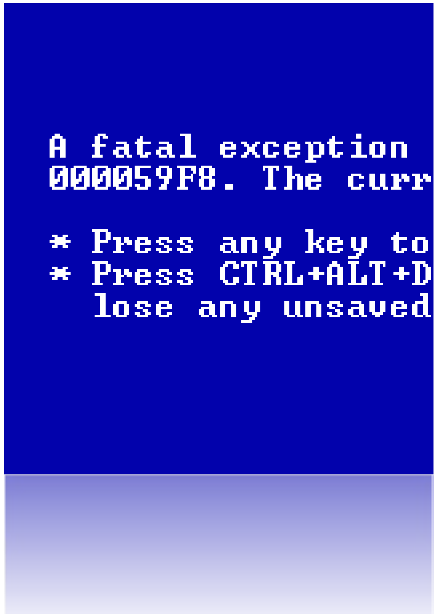
Operational risk

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



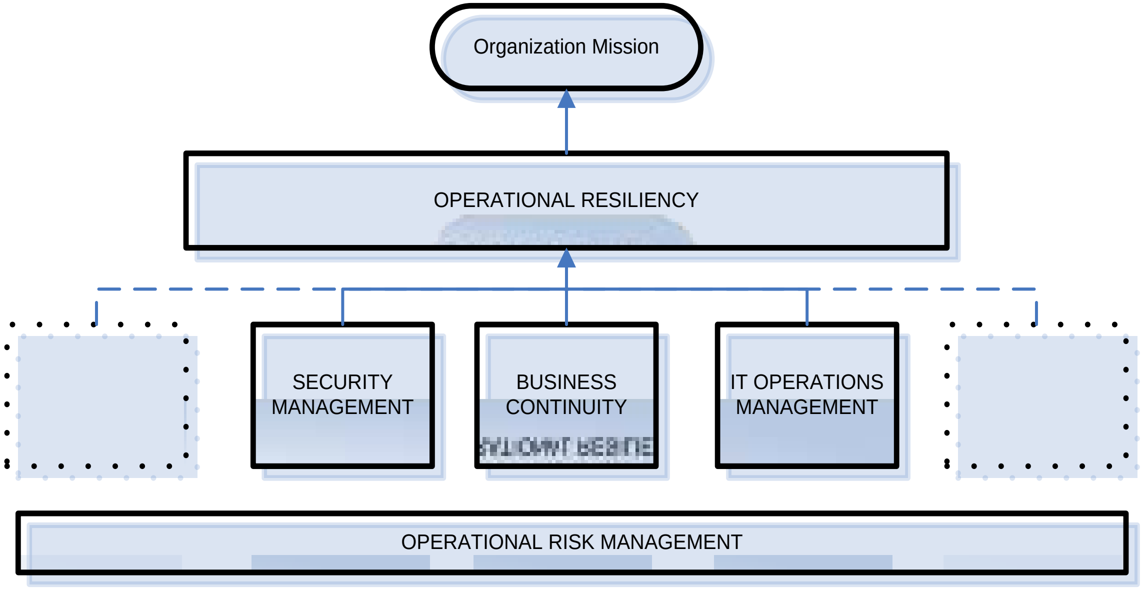
```
A fatal exception
000059F8. The curr

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

Failed internal processes

External events

Operational resiliency and convergence



Convergence directly affects the level of operational resiliency.

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

CERT® Resiliency Management Model

Capability maturity model—guidelines and practices for

- Converging of security, business continuity, and IT ops
- Achieving, managing, and sustaining operational resiliency
- Managing operational risk through process
- Measuring and maturing the resiliency process

Focuses on “what” not “how”

Organized into 26 process areas

Common vernacular and basis for objective appraisals

www.cert.org/resiliency

The Building Blocks of Resiliency Engineering

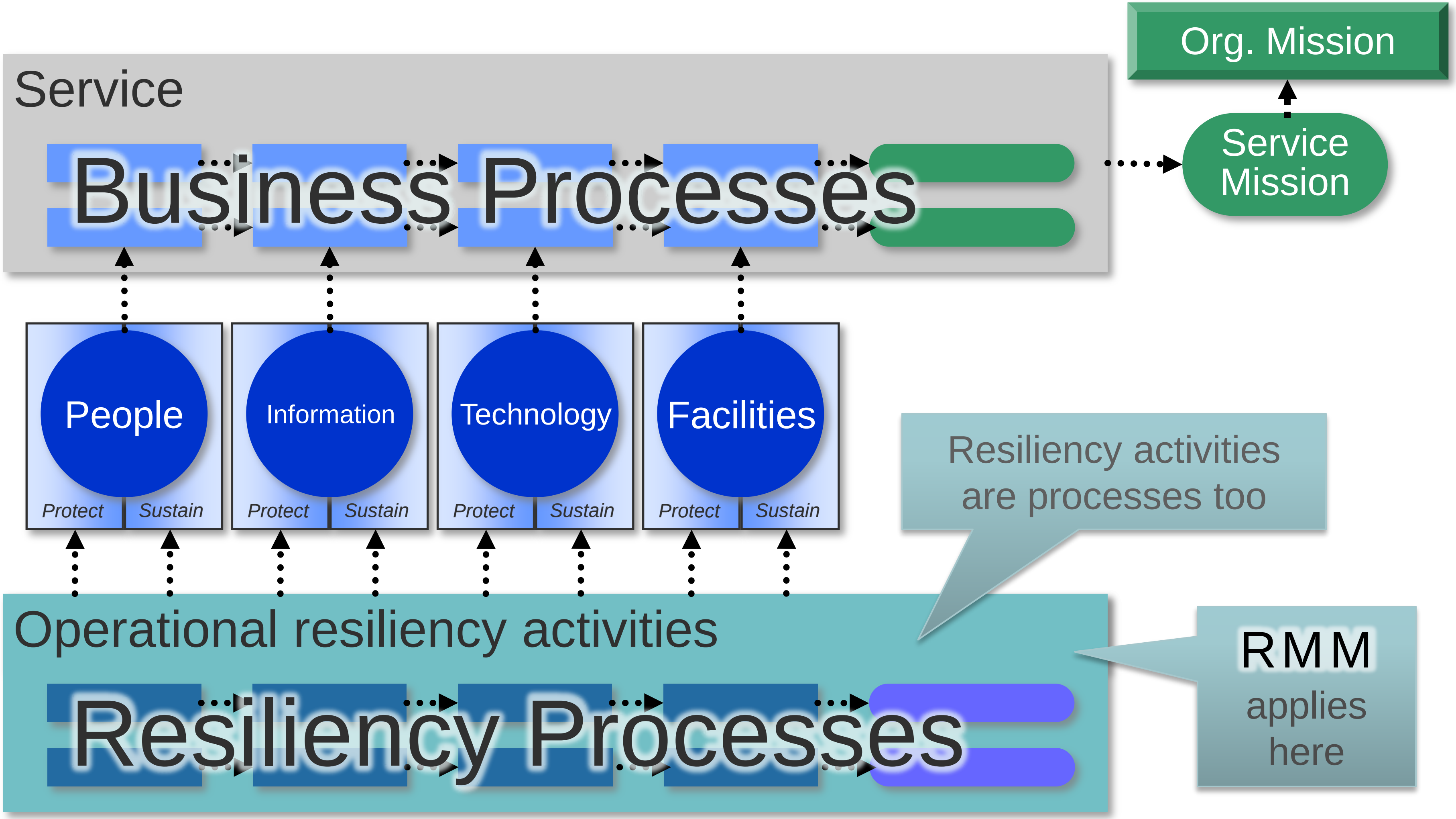
Resiliency engineering

The process by which an organization establishes, develops, implements, and manages the operational resiliency of services, related business processes, and associated assets

Includes both development (build-in) and operational (manage) aspects

Actualizes the concepts of convergence and operational resiliency management

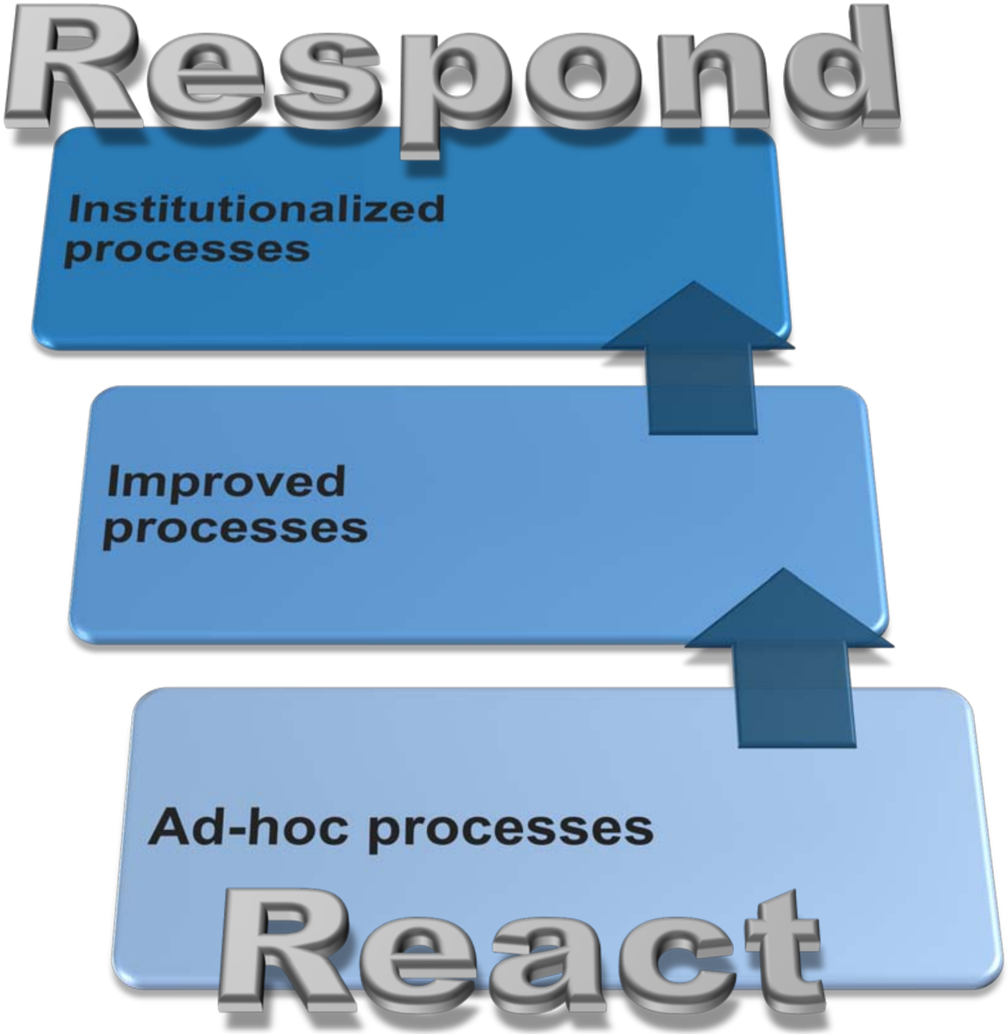
Enterprise view of resiliency management -2



Resiliency activities are processes too

RMM applies here

Resiliency process maturity matters

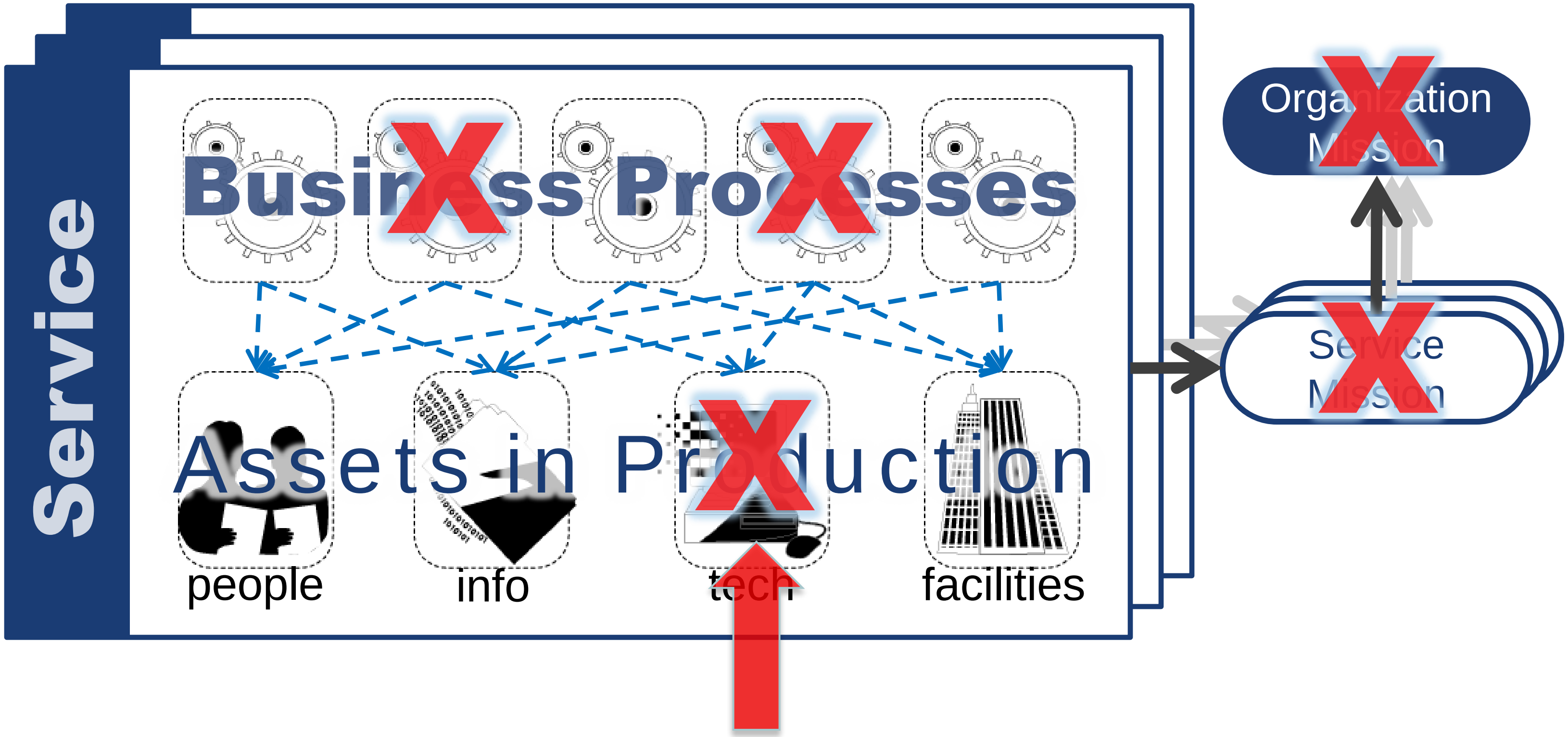


Higher maturity improves

- Predictability
- Sustainability
- Consistency

Process maturity is predictive of future performance — an indicator of the sustainability of the resiliency processes

Organizational context - disruption



Operational risk can disrupt an asset

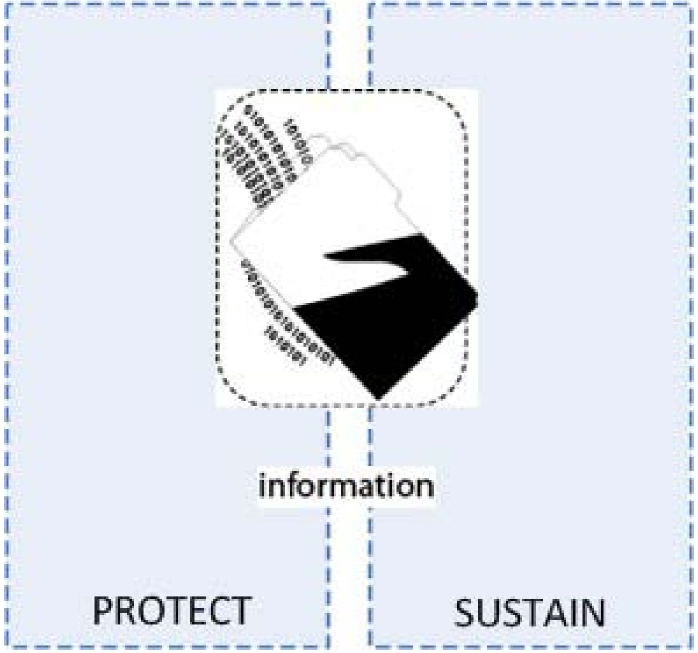
And lead to organizational disruption

Operational resiliency starts at the asset level

To ensure operational resiliency at the **service level**, related assets must be

- Protected from threats and risks that could disable them
- Made sustainable under adverse conditions

The optimal "mix" of these strategies depends on the **value of the asset** and the **cost of deploying and maintaining the strategy.**



Resiliency requirements -1

The requirements for protecting and sustaining an asset in the context of its operational use and constraints

Establish a foundation for how the asset must be protected and sustained to ensure operational resiliency of services to which the asset is associated

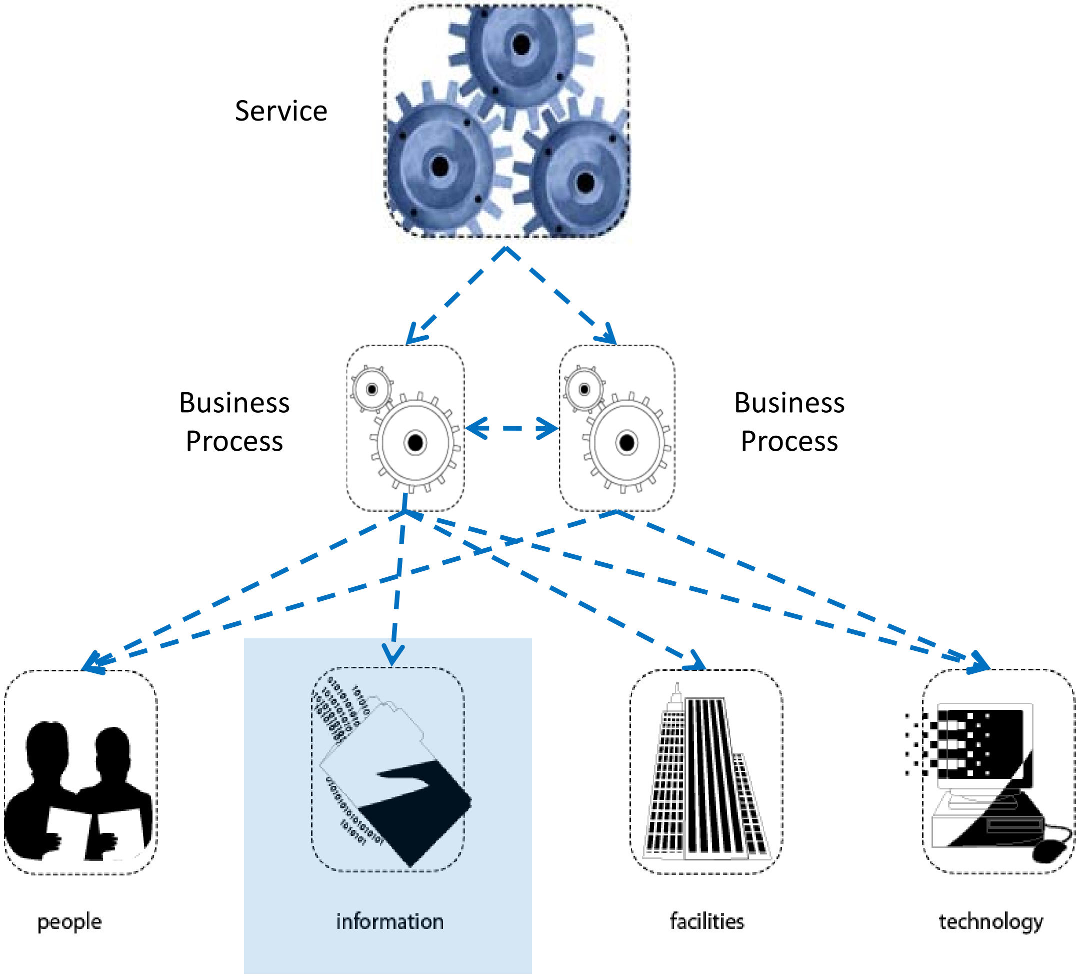
Formed around traditional “information security” categories of confidentiality, integrity, and availability

Failure to meet requirements may impact operational resiliency.

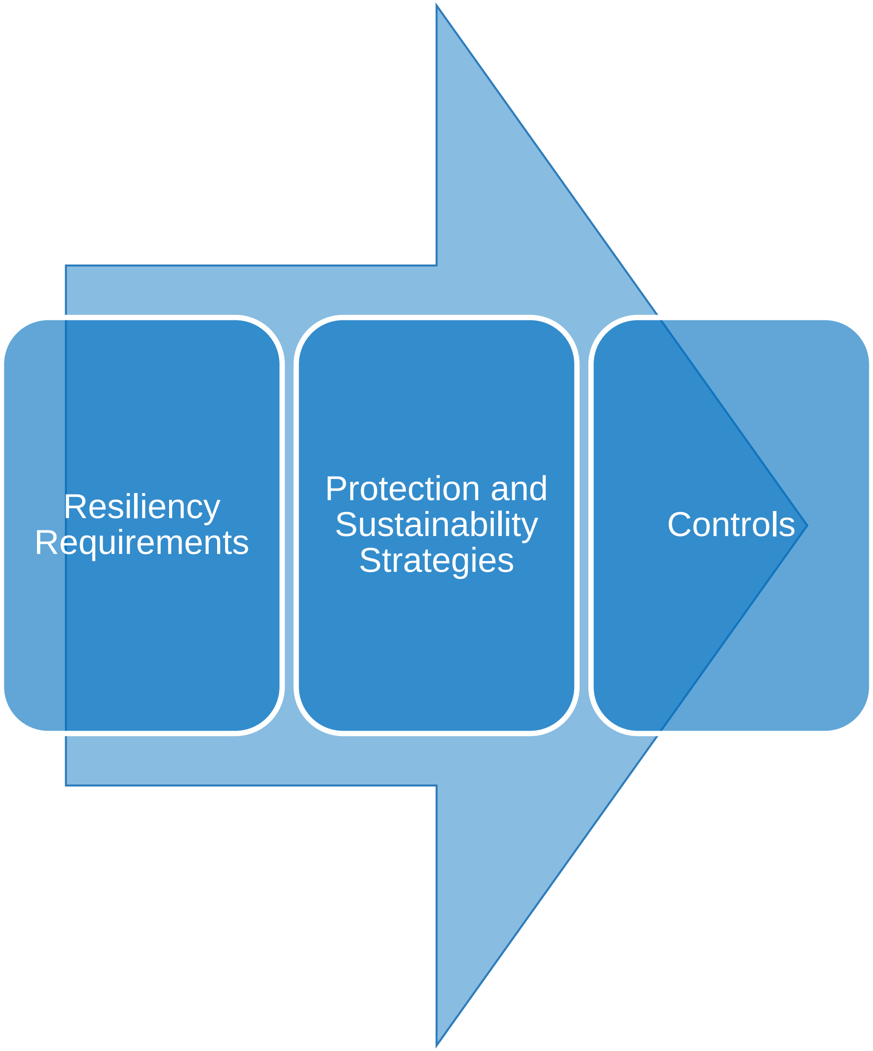
Resiliency requirements -2

In the case of information—if the **integrity** requirement is compromised, the information may not be usable in the form intended, thus impacting associated business processes.

Or, if unintended changes are made to the information (compromise of **integrity**), it may cause the business process to produce unintended results.



From requirements to controls



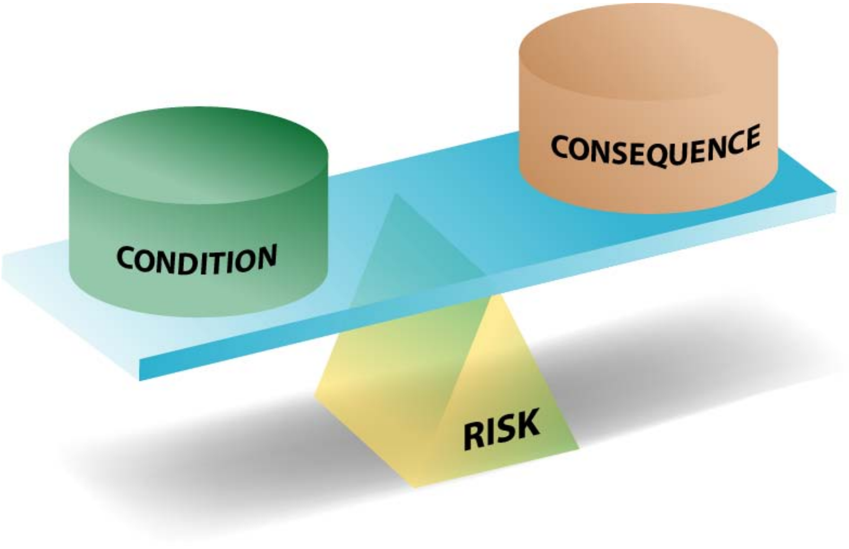
Resiliency requirements form the basis for protection and sustainability strategies.

Protection and sustainability strategies determine the type and level of controls needed to ensure operational resiliency.

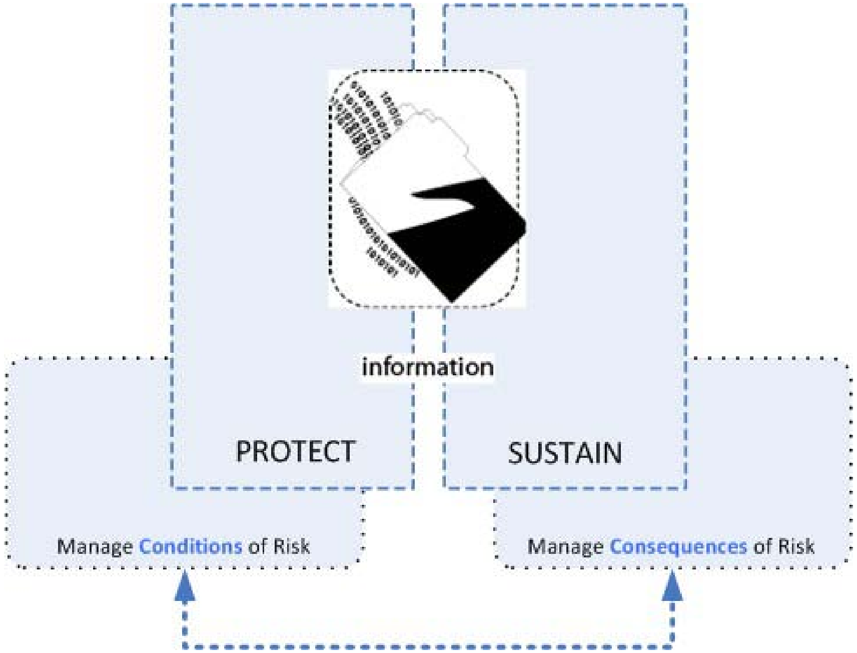
These controls must satisfy the requirements.

Protection, sustainability, and risk

Basic risk equation



Protection & sustainability

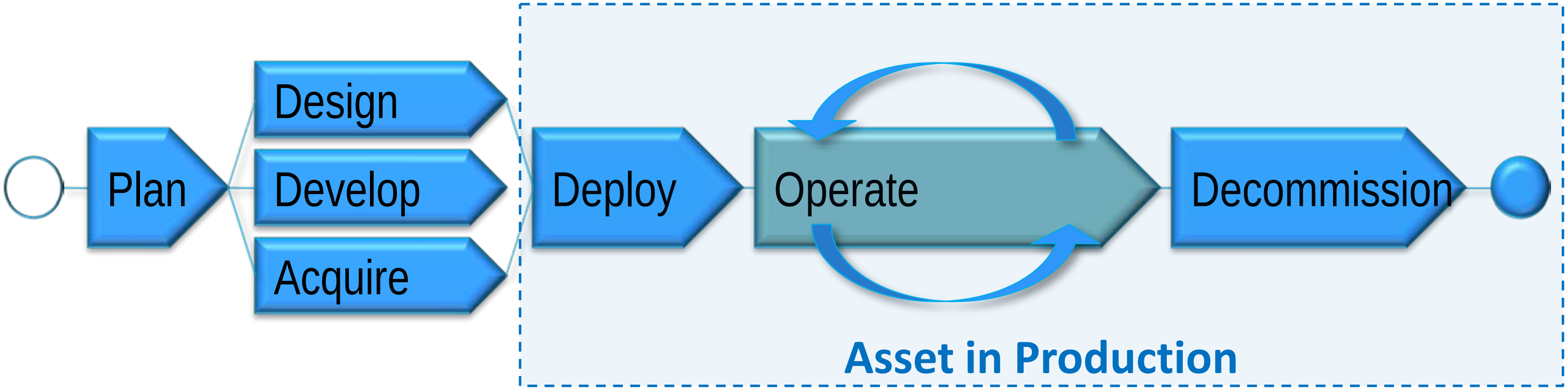


Operational resiliency requires balancing these strategies in a way that minimizes operational risk (to the associated services) and is resource efficient: **the management challenge of operational resiliency**

Resiliency engineering in the life cycle

Resiliency engineering covers the life cycle of an asset.

Operational resiliency management focuses on the deploy, operate, and decommission phases.



Introducing the CERT® Resiliency Management Model

A managerial challenge

Achieving and sustaining an acceptable level of operational resiliency is a **managerial** challenge.

There are certainly technical aspects to the challenge, but coordination, cooperation, and convergence are required.

The organization must have established **processes** to ensure that

- all of the resiliency engineering building blocks are deployed toward the same objectives
- work related to managing operational resiliency is planned, executed, managed, measured, and improved

Success factors

To manage this environment, an organization must be successful at:

- Communicating mission and strategic directives
- Providing guidance on risk appetite to risk-based activities
- Eliminating silos and organizational barriers
- Promoting convergence between operational risk activities
- Optimizing protection and sustainability strategies
- Defining and communicating operational resiliency management processes
- Planning, executing, and managing operational resiliency management work tasks
- Baselining and measuring progress

Doing vs. managing

Most organizations have experience at the tactical level

- Significant body of **codes of practices** to guide effort
- Significant range of available **technology solutions**
- Practitioners' **skill levels** have matured significantly

BUT—very few organizations are skilled at **managing the process** so that it

- is effective, efficient, optimal, and meets stated objectives
- can produce reliable and predictable results now, **and**
  - under times of stress
  - under uncertain conditions, or
  - when the risk environment changes

Today vs. tomorrow

A limiting factor for many organizations is that they cannot repeat their successes.

Performance today is not an adequate predictor of performance tomorrow.

“How am I performing today?” is the wrong question to ask.

The right question is “Do I have what it takes to sustain high performance beyond today?”

Developing a solution

In developing a solution to help organizations manage operational resiliency effectively, two critical elements were identified:

1. The ability to define the **range of activities** required to manage operational resiliency
2. The ability to measure the degree to which an organization is positioned to **sustain their managerial capabilities**

CERT® Resiliency Management Model -1

A **process improvement model** for managing operational resiliency

A **maturity model** with a capability dimension to measure process institutionalization

Promotes the **convergence** of security, business continuity, and IT operations activities as a means to actively direct, control, and manage operational resiliency and risk

A **guide** for improving the process of managing operational resiliency and deploying practices effectively

A **unifying factor** for terminology, process definition, and objective benchmarking and appraisal

CERT® Resiliency Management Model -2

Critical elements of the “solution” are satisfied in the model

1. **Range of activities** instantiated in 26 process areas
2. **Sustaining managerial competency** instantiated in capability maturity overlay

Distinguishing features of RMM

Embodies the **convergence** principle in the process definition

Descriptive rather than **pre**scriptive—focuses on the “what” not the “how”

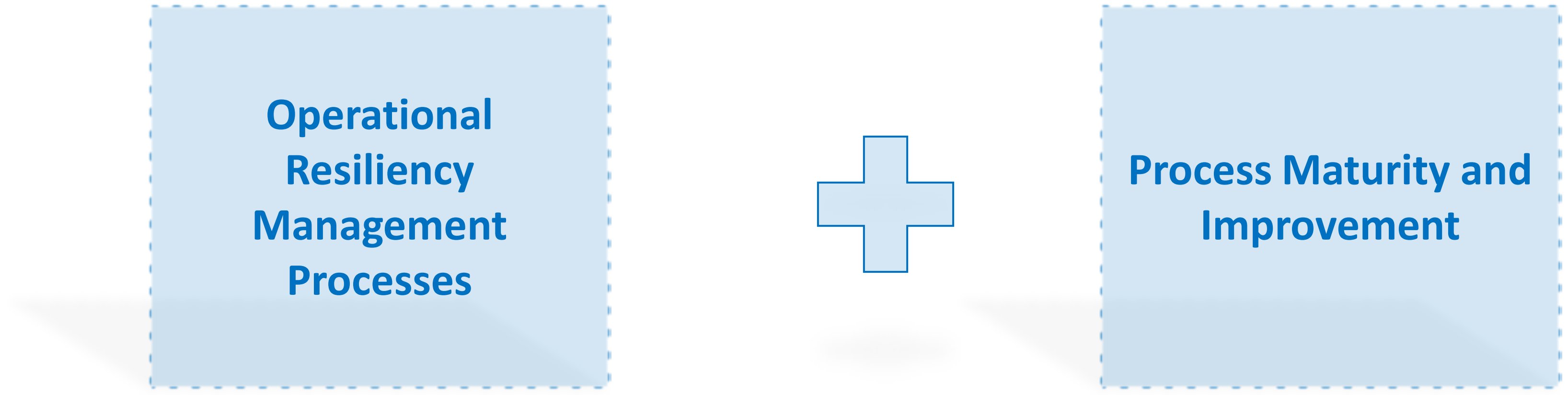
Provides an **organizing convention** for effective selection and deployment of codes of practice

Introduces the **process maturity** concept to support process improvement

Provides a basis for **consistent and quantitative measurement** of effectiveness

Not a proprietary model—benefits from experience of community and SEI stewardship

Combining approaches



Operational Resiliency Management Processes

Process Maturity and Improvement

RMM combines a **convergent approach to managing operational resiliency** with a **model-based approach to establishing, measuring, and improving processes.**

Value of the process maturity dimension -1

The process maturity dimension has been transformative in other disciplines.

In software engineering, the process maturity dimension speaks to the organization’s ability to produce high-quality work products consistently and repeatedly.

“The quality of a system or product is highly influenced by the quality of the process used to develop and maintain it.”[1]

The **predictability** factor increases relative to how the organization will perform over time—especially important to managing operational resiliency in uncertainty.

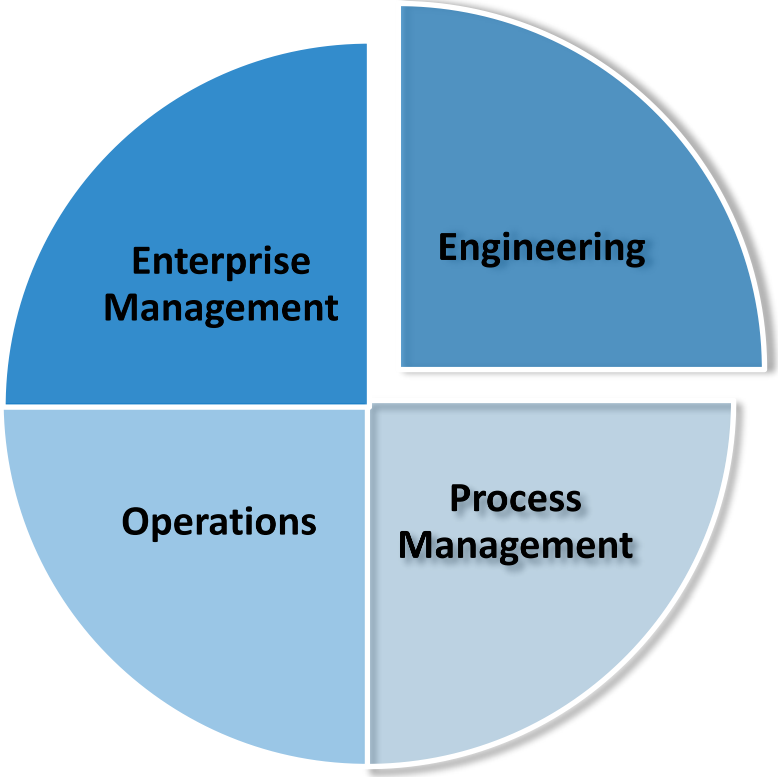
[1] *Source: CMMI® for Development, Version 1.2, CMU/SEI-2006-TR-008, Software Engineering Institute, Carnegie Mellon University, August 2006*

RMM model architecture

Comprised of 26 process areas across four categories

1. Enterprise management
2. Engineering
3. Operations management
4. Process management

Arranged in a continuous representation—no staged guidance on adoption



RMM at a glance

Requirements Management

RRD – Resiliency Requirements Development

RRM – Resiliency Requirements Management

Asset Management

ADM – Asset Definition and Management

Establishing Resiliency

SC – Service Continuity

CTRL – Controls Management

RTSE – Resilient Technical Solution Engineering

Governance, Risk, & Compliance

COMP – Compliance

EF – Enterprise Focus

RISK – Risk Management

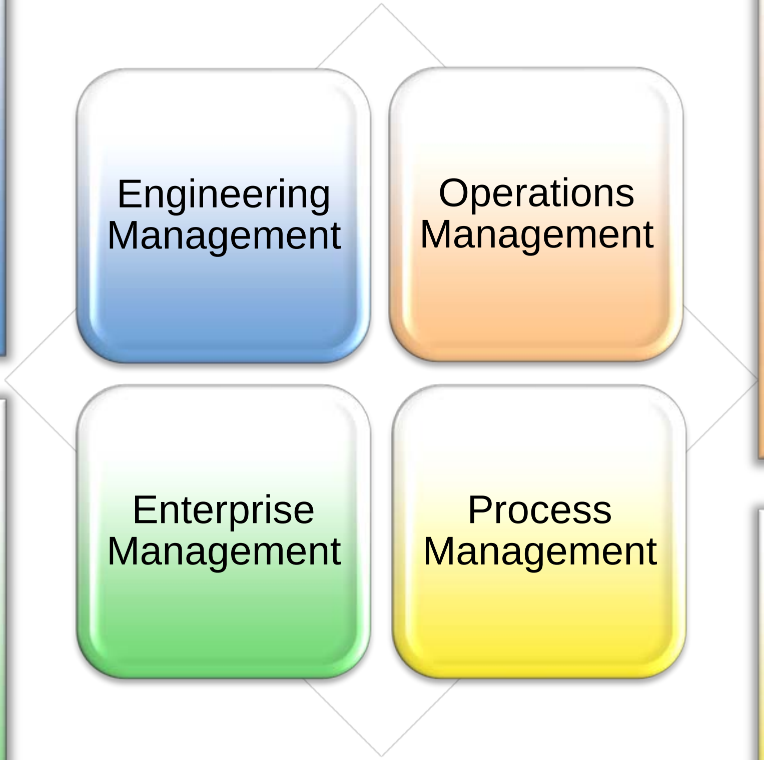
Supporting Resiliency

COMM – Communications

FRM – Financial Resource Management

HRM – Human Resource Management

OTA – Organizational Training & Awareness



Engineering Management

Operations Management

Enterprise Management

Process Management

Asset Resiliency 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

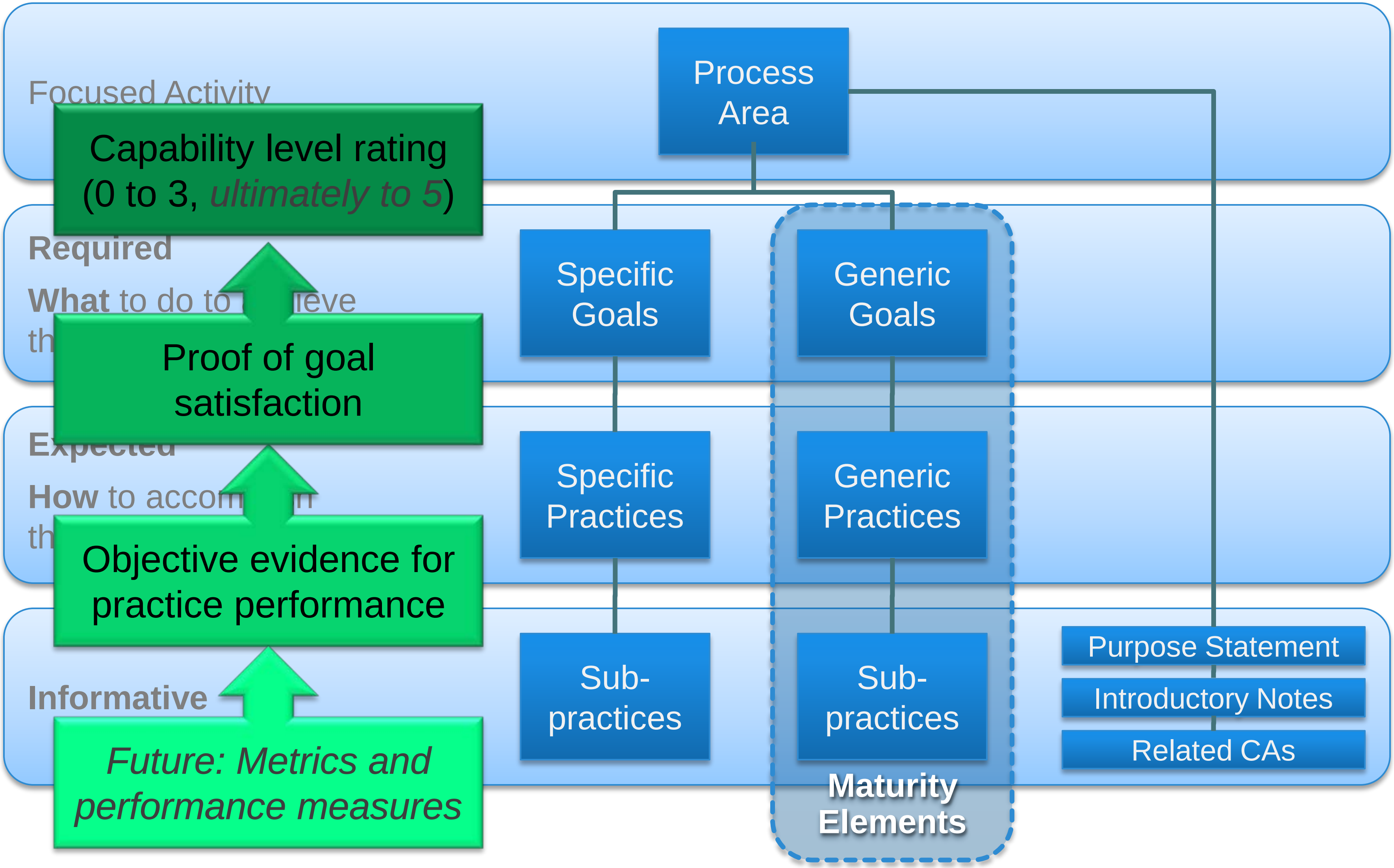
Process Management

MA – Measurement and Analysis

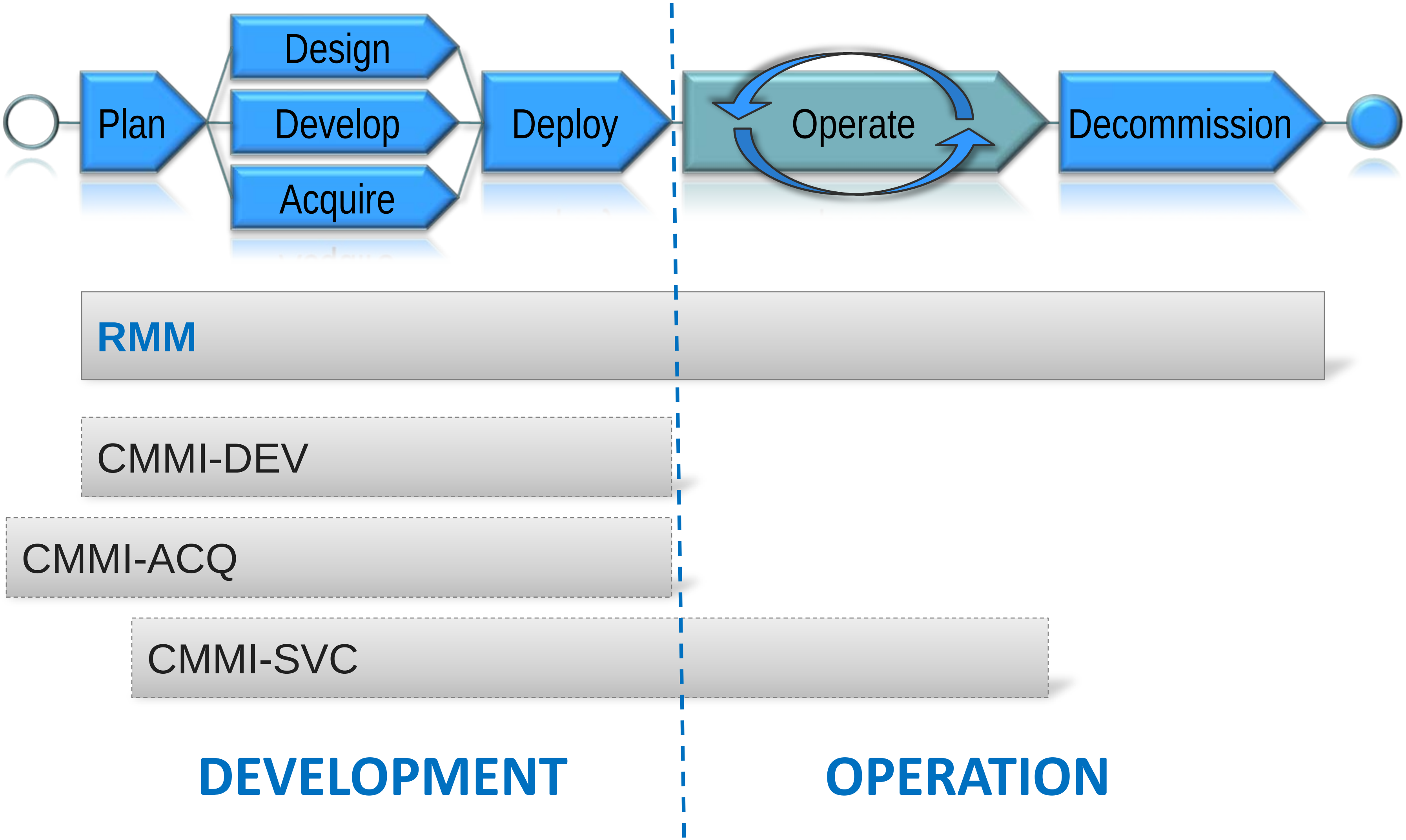
OPD – Organizational Process Definition

OPF – Organizational Process Focus

Process Area Structure & Evidence context



RMM position in lifecycle



Plan

Design

Develop

Acquire

Deploy

Operate

Decommission

RMM

CMMI-DEV

CMMI-ACQ

CMMI-SVC

DEVELOPMENT

OPERATION

RMM product suite

Model

Appraisal methodology based on SCAMPI

Introductory courses

- Model training
- “How-to” courses
- Executive workshops

Advanced courses

- Practitioner training
- Appraisal leader training
- Instructor training

RMM – Today

First class A RMM appraisal recently completed

Working with DHS and other Federal agencies to position RMM for resiliency management in the civilian agencies

Continuing to support adoption in the financial industry in collaboration with FSTC

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

Framework version 1.0 release
(in process at www.cert.org/resiliency)

Public Intro courses available

Summary

RMM is built on the principle of convergence of operational risk management activities.

The building blocks of resiliency engineering include services, business processes, assets, resiliency requirements, protection and sustainability strategies, and controls.

RMM contains 26 process areas that embody the range of resiliency activities and a capability maturity overlay.

RMM is focused in operations but reaches back into development processes.

RMM can be deployed relative to the organization’s objectives.

Questions?

Notices

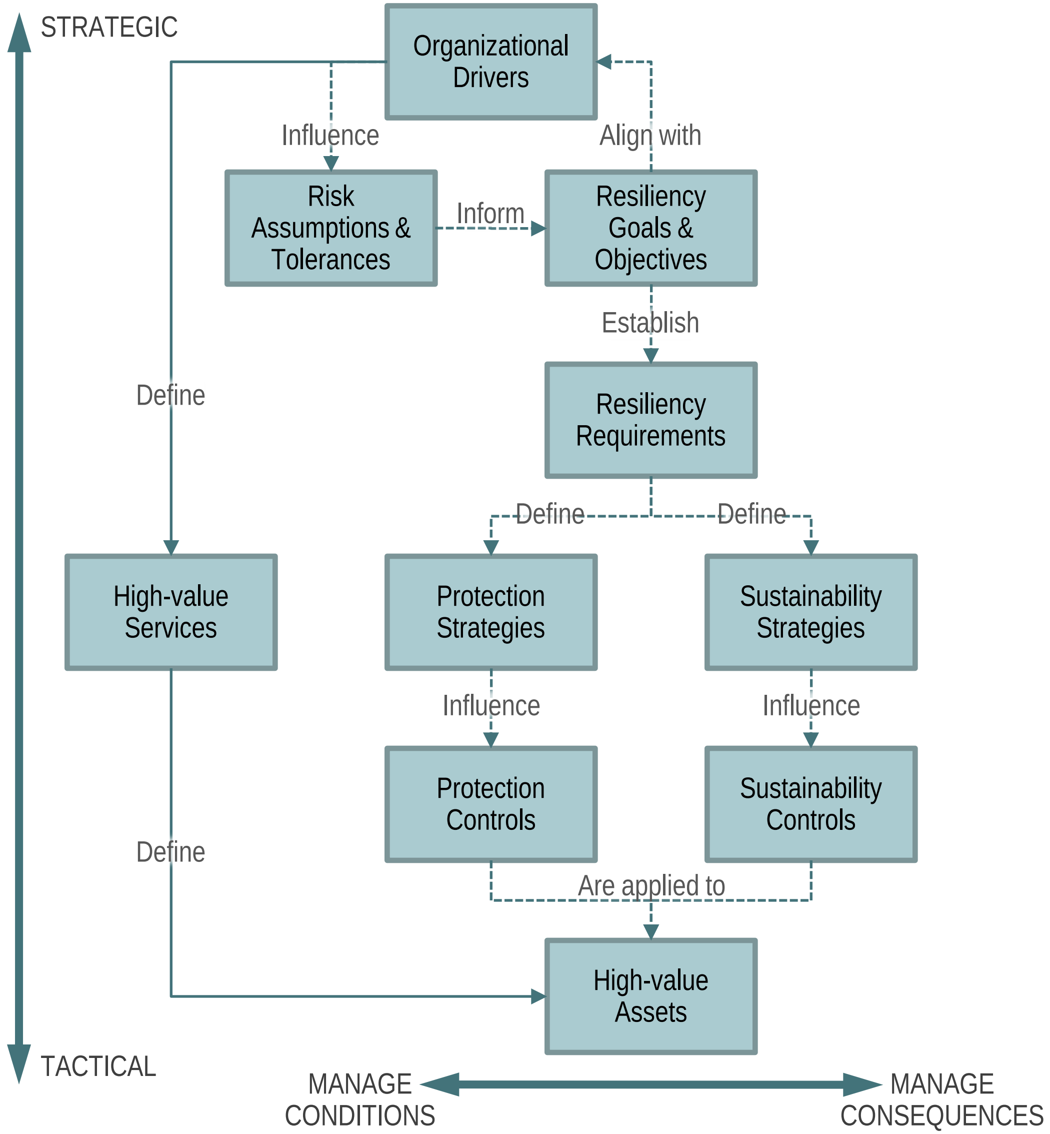
Extra Material

The environment at 30,000 feet

This is the environment that the organization must manage effectively and efficiently.

The environment that needs to be managed is not static.

Technology is not the driving issue.



Services

The limited number of activities that the organization performs to deliver a service or to produce a product

Can be internally-focused (i.e., administrative or support)

Can be externally-focused (i.e., producing widgets for customers)

Typically align with a particular organizational unit, but can cross units and organizational boundaries

Service mission must enable the organization's mission—otherwise, why would you perform it?

Business processes

The activities that the organization (and its suppliers) perform to ensure that services meet their mission

Traverse the organization—cross organizational lines

Often are performed outside of the boundaries of the organization

A **service** is made up of one or more **business processes.**

Business process mission must enable service mission.

Assets

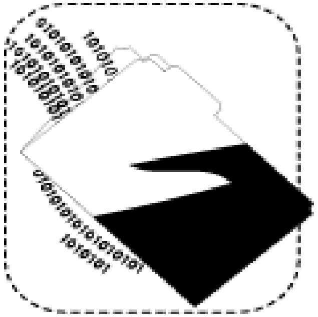
Something of value to the organization

“Charged into production” of business processes and services

Asset value relates to the importance of the **asset** in meeting the **business process** and **service** mission.

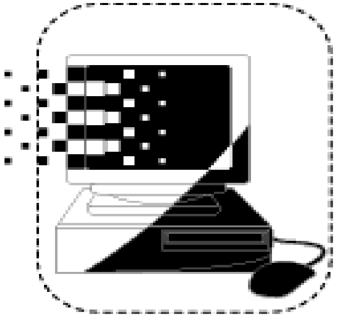
Assets

people



information

facilities

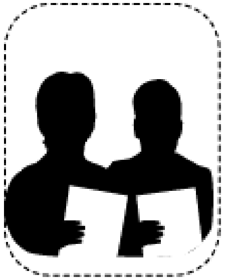


technology

Four types of assets are the focus of resiliency engineering as defined in RMM. These include **people, information, facilities, and technology.**

Note: other assets may be important to operational resiliency, such as raw materials (steel, water, etc.)

People

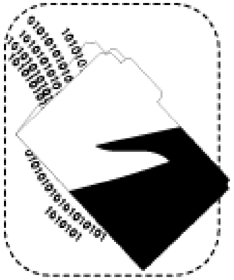


The human capital of the organization

Use the other resiliency assets to plan, execute, and manage work products

Subject to the **availability** requirement

Information



information

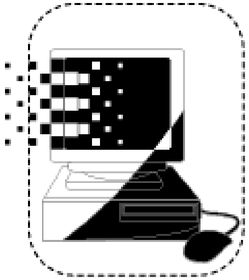
A collection of related data or knowledge vital to the performance of a service or business process

Can be in electronic or physical form

May be “intellectual capital”

Subject to **confidentiality, integrity, and availability** requirements

Technology



technology

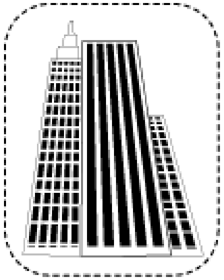
Any technology component that supports or automates a business process and facilitates its ability to achieve its mission

Can include software, systems, and hardware, or combinations thereof

Pervasive across all functions of the organization

Subject to **integrity and availability** requirements

Facilities



facilities

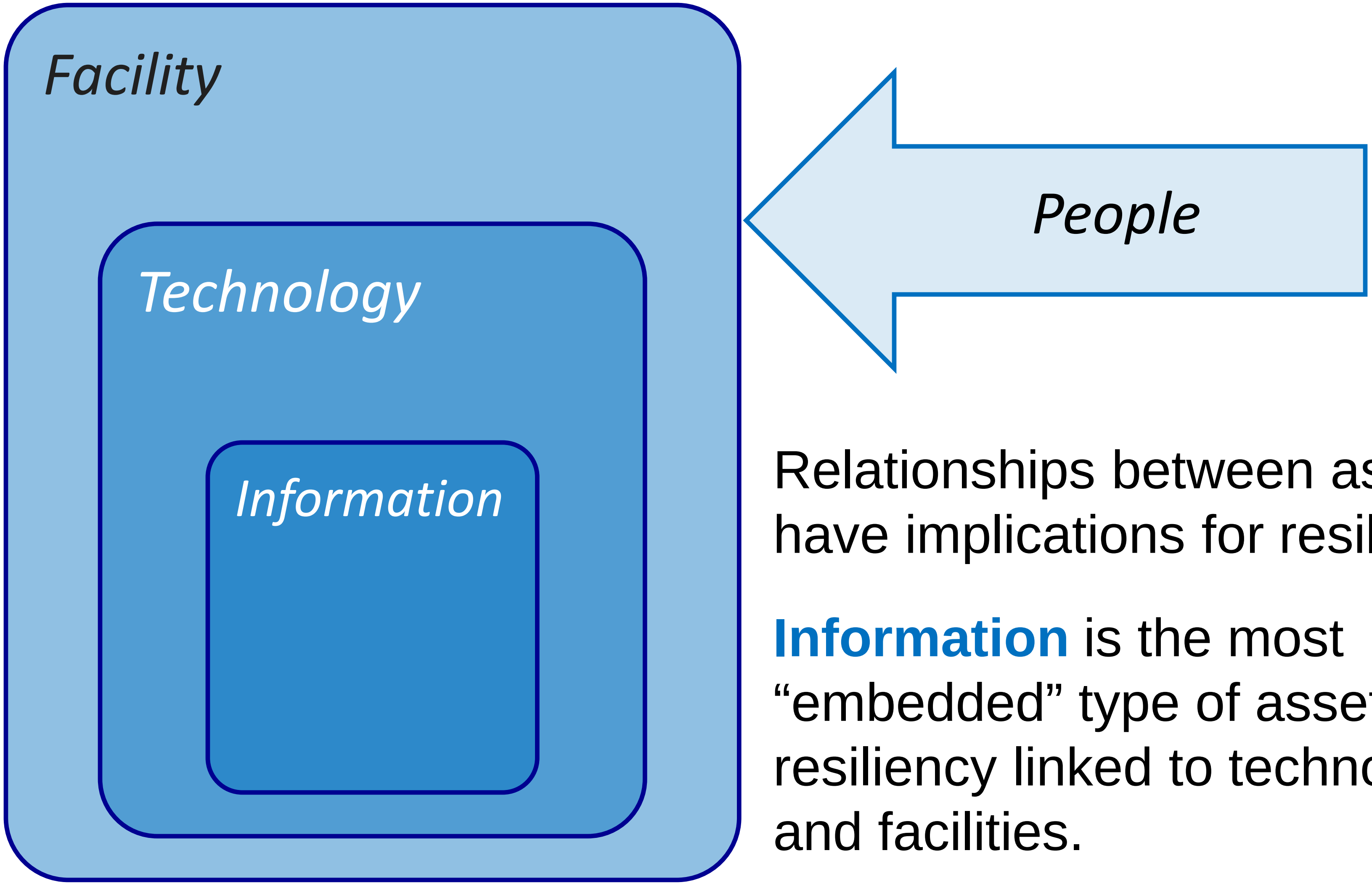
Any physical plant asset that the organization relies upon to execute a service

The physical places where other resiliency assets “live”

Provides direct support for business process achievement

Subject to **integrity and availability** requirements

Putting assets in context



Relationships between assets have implications for resiliency.

Information is the most “embedded” type of asset—resiliency linked to technology and facilities.

Overlap between RMM & CMMI process areas

RMM Process Area		Equivalent or Related CMMI PA	
RISK	Risk Management	**RSKM**	Risk Management
MA	Measurement and Analysis	**MA**	Measurement and Analysis
RRD	Resiliency Requirements Development	**RD**	Requirements Development
RRM	Resiliency Requirements Management	**RM**	Requirements Management
OTA	Organizational Training and Awareness	**OT**	Organizational Training
OPD	Organizational Process Definition	**OPD**	Organizational Process Definition
OPF	Organizational Process Focus	**OPF**	Organizational Process Focus
RTSE	Resilient Technical Solution Engineering	**TS**	Technical Solution