Sustaining Operational Resiliency: A Process Improvement Approach to Security Management

Rich Caralli

Carnegie Mellon University Software Engineering Institute

Bank Security Summit June 2006

Background

Why is security a burden to the organization?

Why is security so difficult to manage in a large enterprise?

Why aren’t we more efficient and effective at reaching security goals?

What is value proposition of security to the organization and can it be improved?

Recent case history -1

Poorly planned and organized security function and roles/responsibilities

No active involvement of business units

No information asset management

Funding model reactive, not strategic

Regulatory drivers not a sufficient driver for success

Recent case history -2

Attaining and sustaining security success difficult

Security is a technical function

Frequent collisions between operational units and organization on security strategy

Searching for magic bullet – ITIL, COBIT, etc.

“Can someone else do this for us?”

Organizational impact

Misalignment of operational and security goals

False sense of accomplishment

Failure to utilize all necessary skills/resources

Compliance at the expense of effectiveness

Static, inflexible approaches

Overall ability to manage security is impaired

Taking a step back

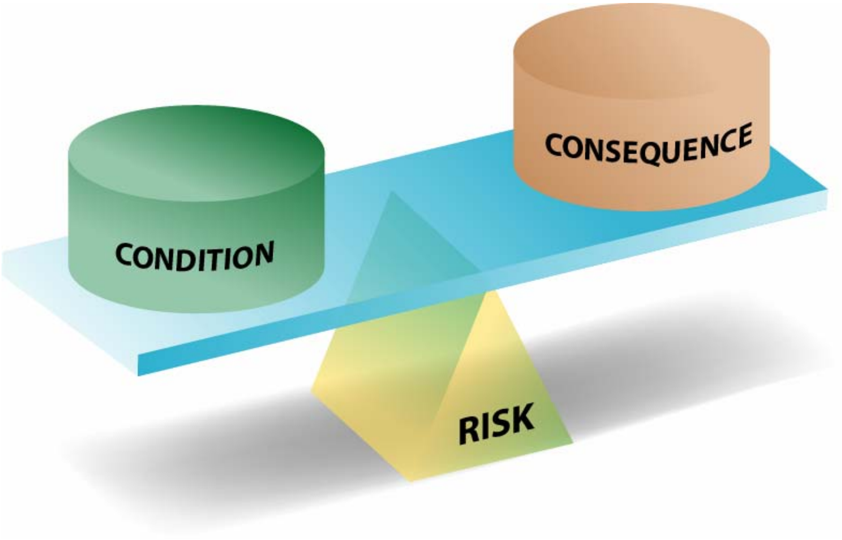
Why do we do “security?”

- Protect critical enterprise assets: information, technology, facilities, and people
- Keep business processes viable
- Minimize disruptions in achieving enterprise goals and mission
- Manage enterprise operational risk

Security is driven by risk. . .

The underlying driver for security is to manage the risk equation:

- Managing firewall rulesets
- Installing access controls to facilities
- Limiting access to intellectual property
- Developing business continuity and disaster recovery plan



All of these activities are in essence about managing operational risk.

Why does it matter?

Organizations must focus their limited resources on identifying and managing the risks that have the most potential to

- disrupt their core business drivers
- impede the survivability of their mission

What is the problem?

Is an organization’s security capability sufficient to identify and manage risks that result from

- failed internal processes
- inadvertent or deliberate actions of people
- problems with systems and technology
- external events

What is the problem?

Is an organization’s security capability sufficient to identify and manage risks that result from

- failed internal processes
- inadvertent or deliberate actions of people
- problems with systems and technology
- external events

Basel II description of operational risk

Evolving security -1

Recognize security as an *operational risk management* (ORM) activity

Focused on keeping critical objects productive – by limiting risk and managing impact of realized risk

Provide value to the organization by *directly supporting operational resiliency*

Enterprise risk management programs rely on ‘point solutions’ and ‘hardening’ instead of layered approaches like defense in depth. Risk management models have not kept pace with these shifts. --Booz-Allen

Evolving security -2

Security alone can’t support and sustain operational resiliency

Security success highly dependent on at least two other activities:

- Business continuity/disaster recovery
- IT operations management

Share responsibility with security for ORM

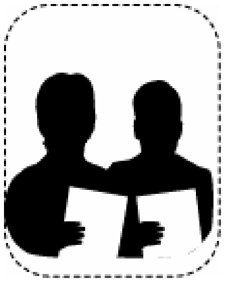
Security management

Focus on keeping critical assets “safe from harm”

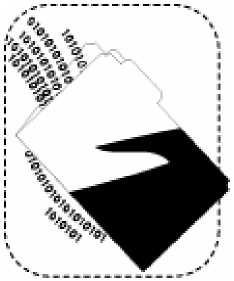
Limiting threats and managing impact

Manage confidentiality, integrity, and availability

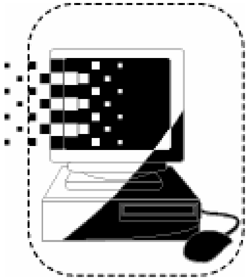
Traverses people, information, technology, and facilities



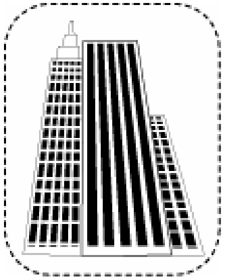
people



information



technology



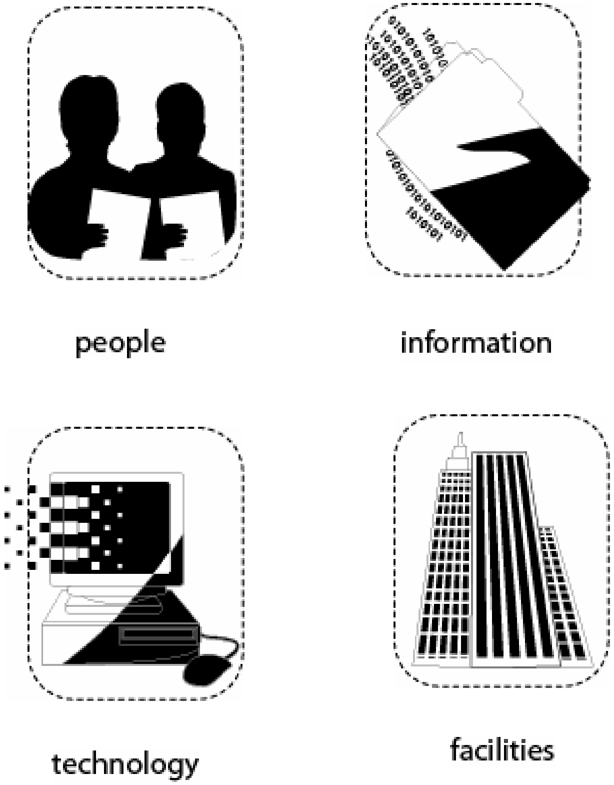
facilities

Business continuity

Limit unwanted effects of realized risk

Ensure availability and recoverability

Focuses on people, information, technology, and facilities

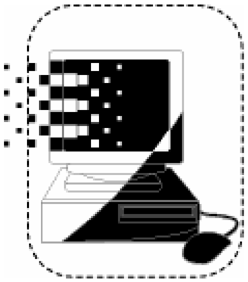


IT operations management

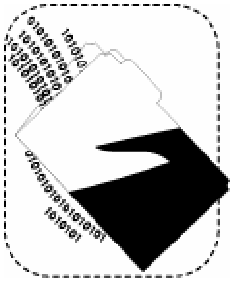
Limit threats that originate in technology infrastructure

Ensure availability and recoverability of technology

Focuses on information and technology



technology



information

A coordinated view

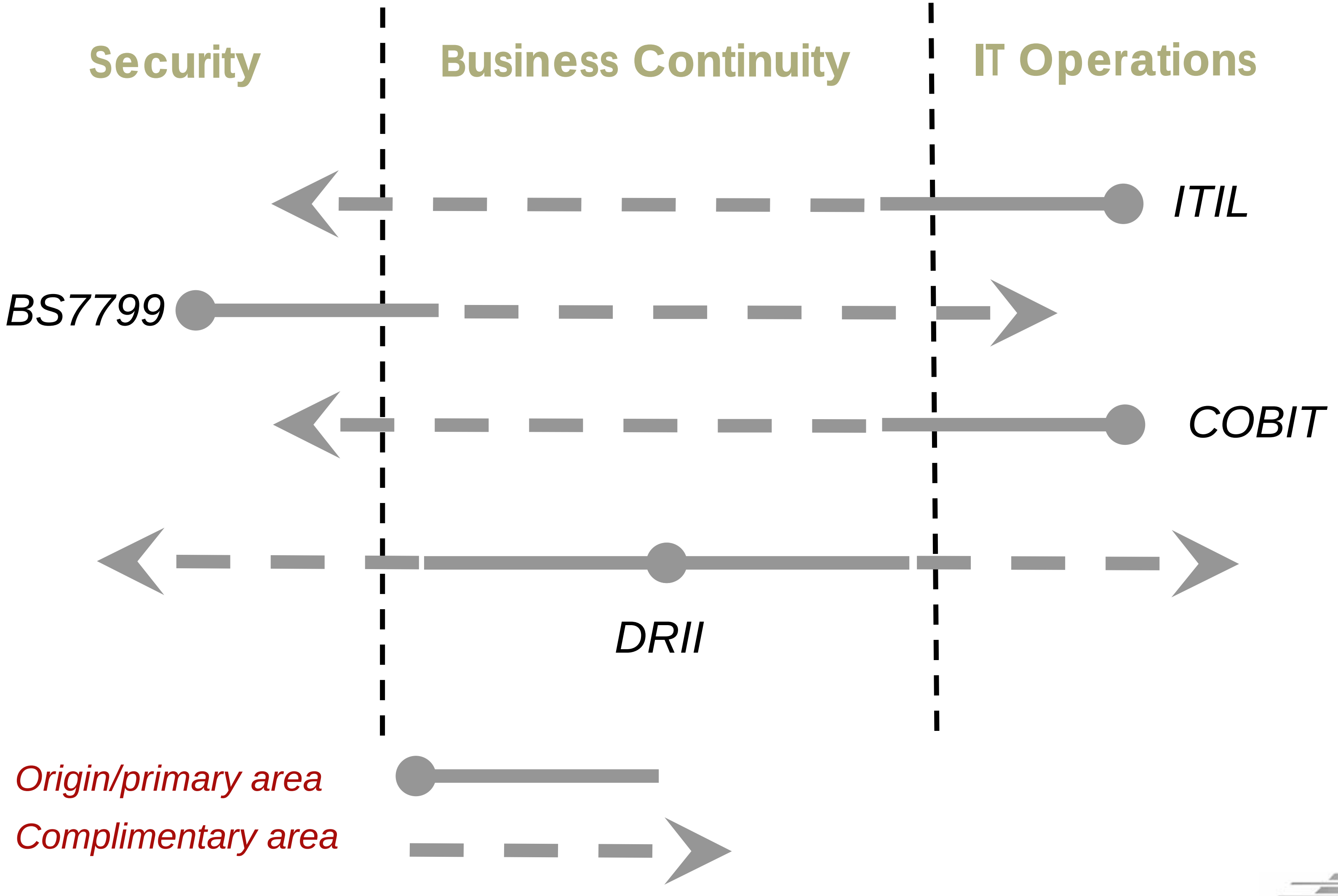
Dependent on each other to complete their missions

Share the same goals, objectives, requirements—driven by organizational needs

Focus on the protection and productivity of the same objects

Rely on shared, common practices

An overlap of practices



Security

Business Continuity

IT Operations

ITIL

BS7799

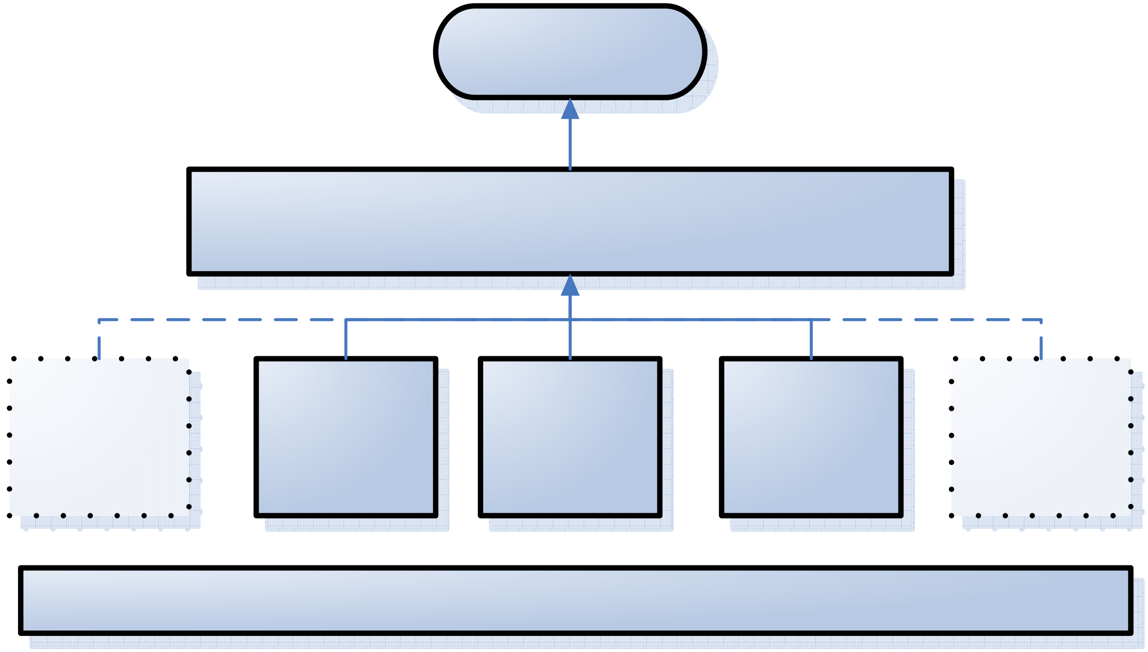
COBIT

DRII

Origin/primary area

Complimentary area

Common goal: operational resiliency



Operational resiliency -1

Managing operational risk to ensure mission viability

Being able to adapt to new risks as they emerge

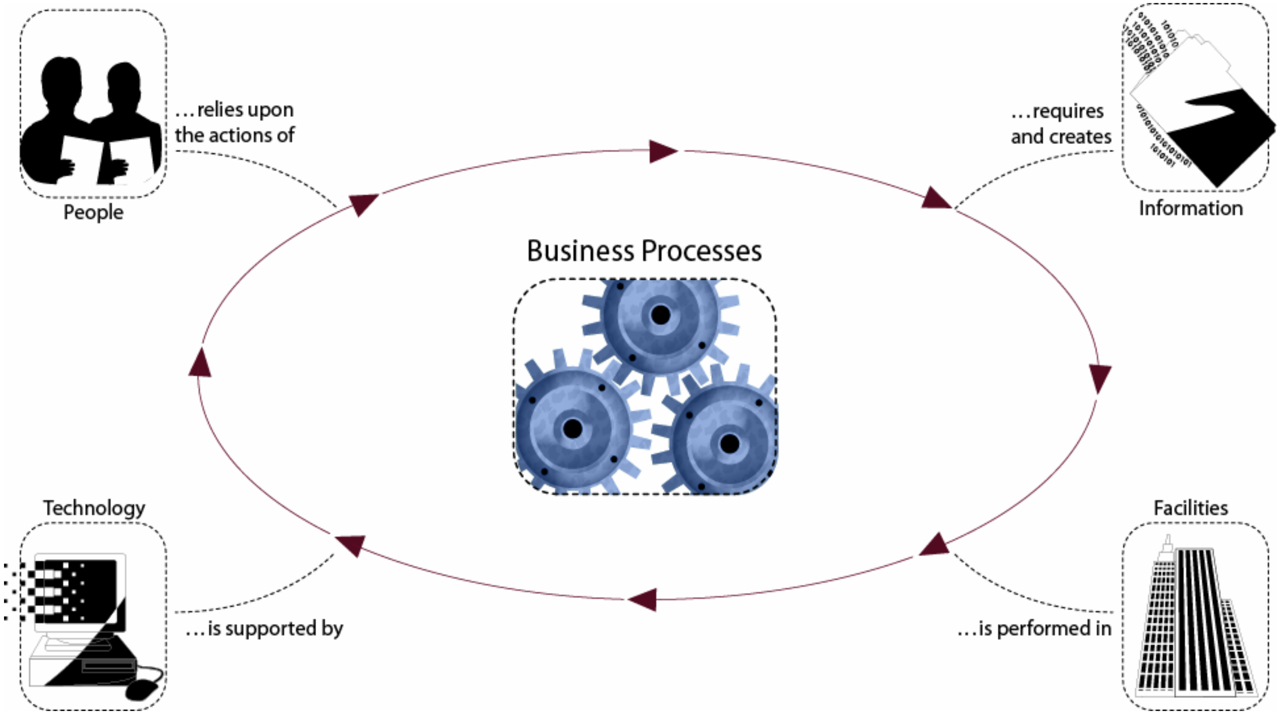
Acting before reacting

"...ability and capacity to withstand systemic discontinuities and adapt to new risk environments" --Booz-Allen

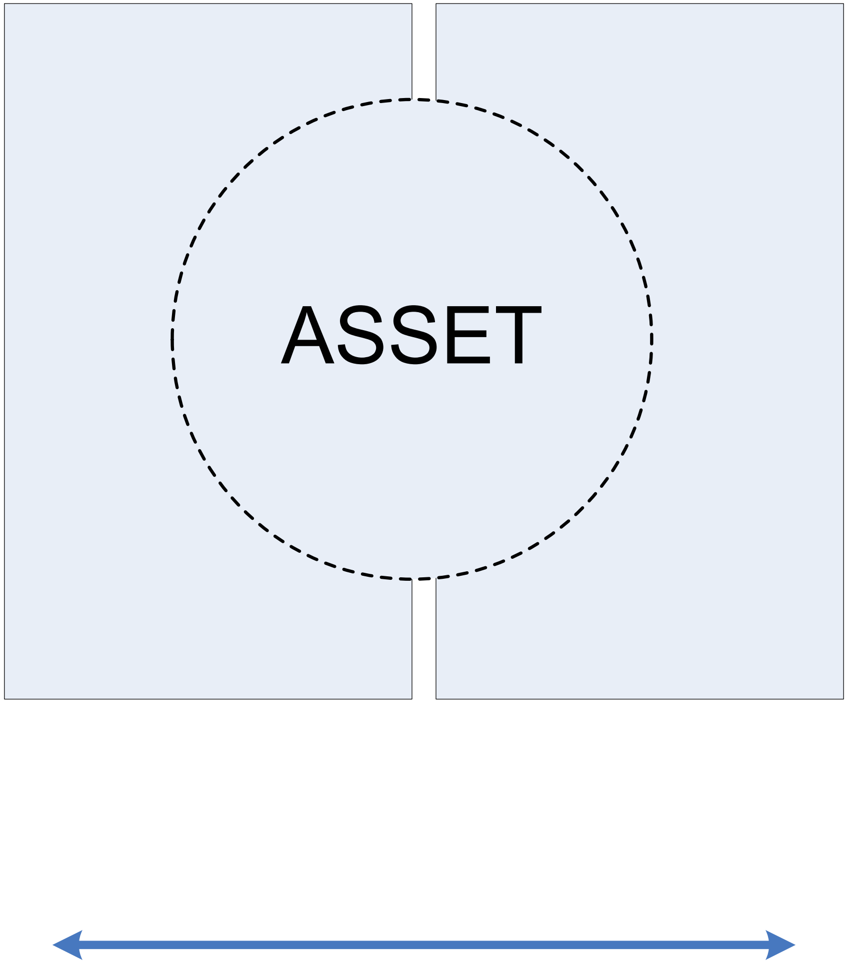
"Adapt to risk before the need becomes desperately obvious." --Harvard Business Review

Operational resiliency -2

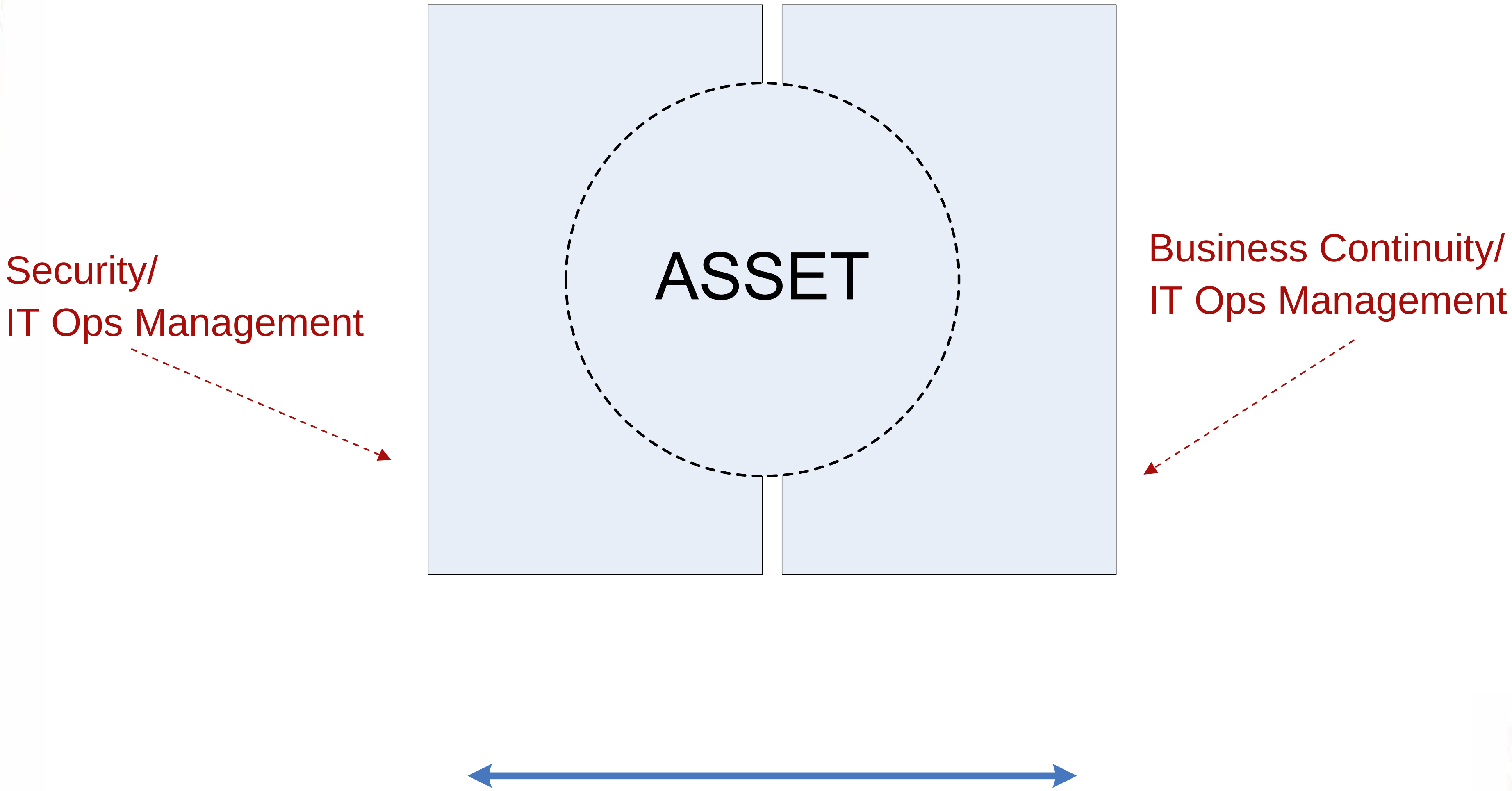
In practice: ensuring the core *critical* objects of the organization function productively as intended



Balanced approach -1



Balanced approach -2

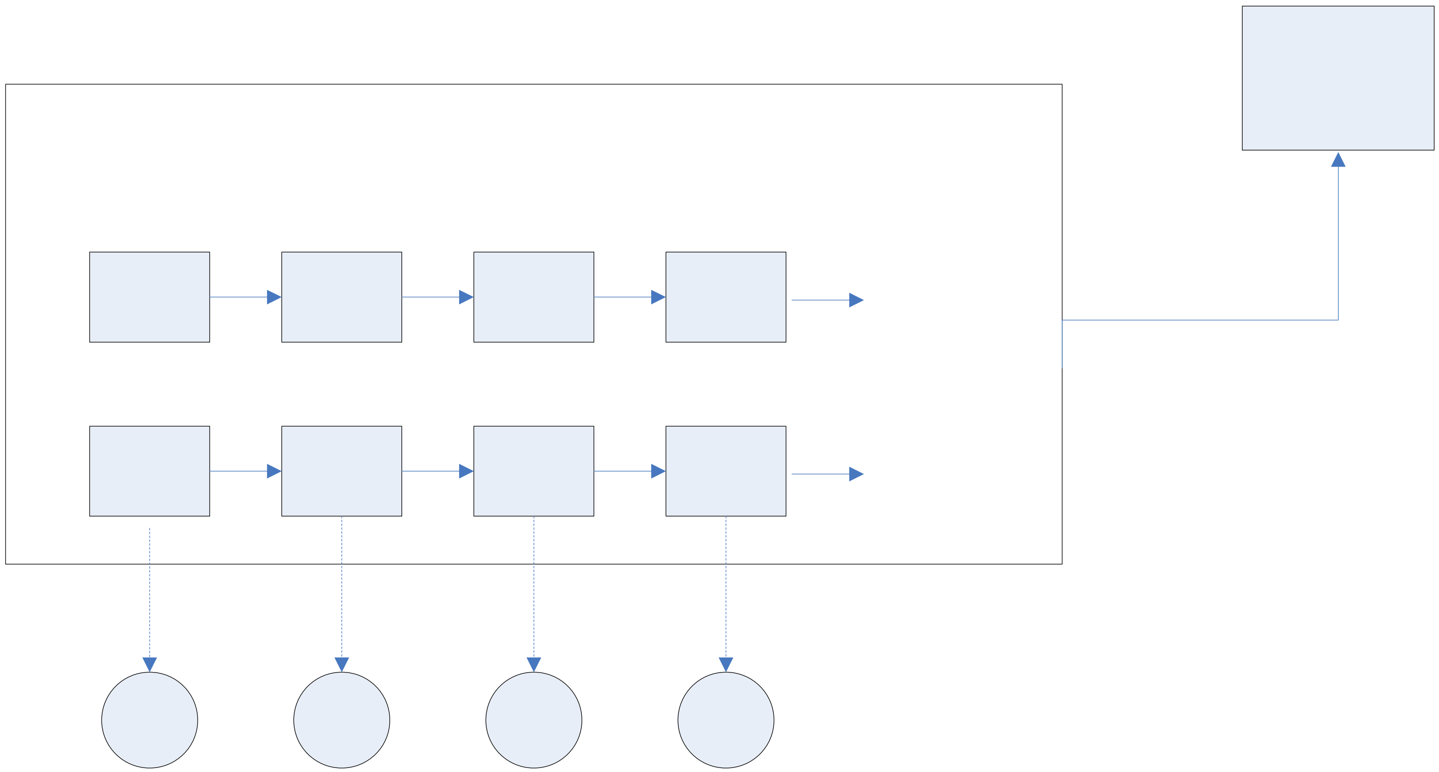


ASSET

Security/
IT Ops Management

Business Continuity/
IT Ops Management

Balanced approach -3



How do we get there?

Organizations not structured today to facilitate collaboration toward common goal

- Funding model
- Management structure and oversight
- Practice-driven
- Compliance focus

Need to view as a definable, manageable process

Considering a process approach

Elevating the management and coordination of operational resiliency-focused activities to the enterprise level.

- Setting and achieving shared goals
- Collaborating and sharing resources
- Eliminating stovepipes
- Eliminating redundancy
- Measuring effectiveness
- Moving toward process improvement

Working smarter, not harder

Why process over practices? -1

Process

Describes the "what"

Set and achieve process goals

Actively manage process to performance requirements

Select practices based on process goals, not on other factors

Practice

Prescribes the "how"

Are there practice goals?

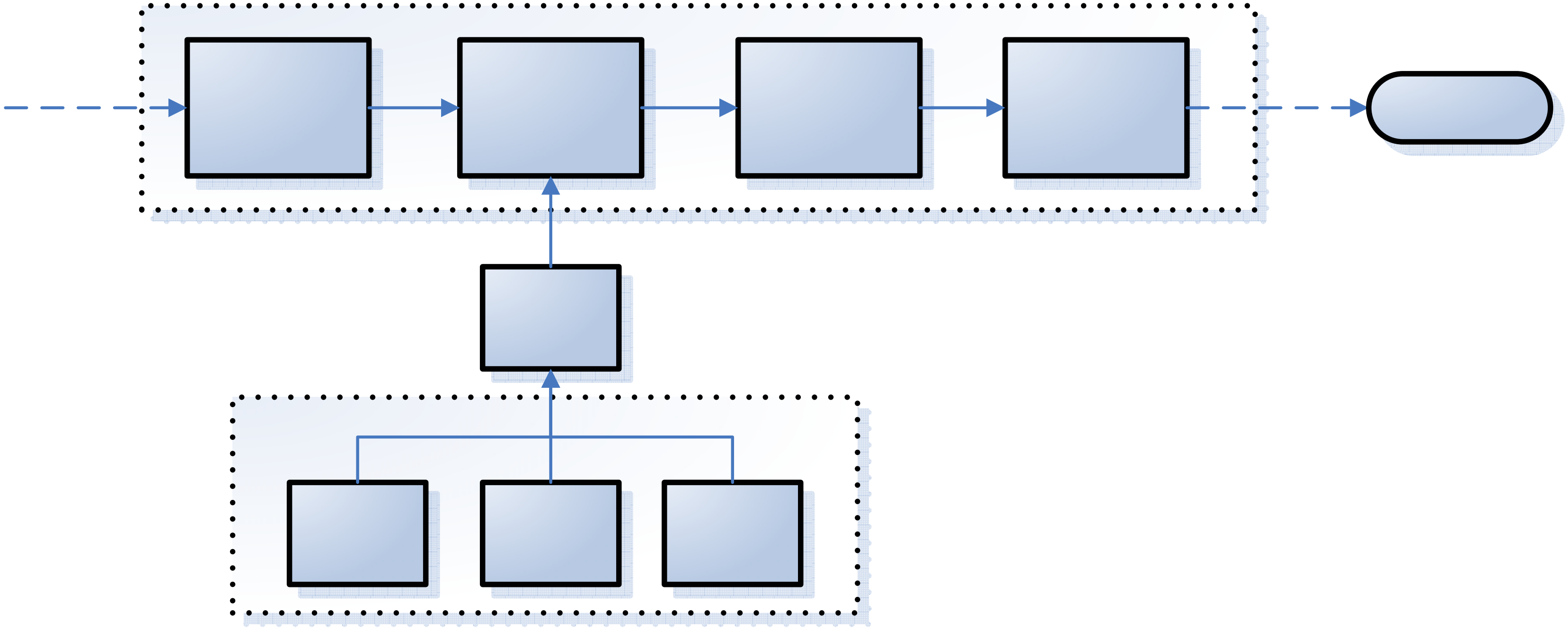
Tends toward "set and forget" mentality

Reinforce domain-driven approach

One size does NOT fit all

Often the vehicle for regulation

Why process over practices? -2



Embracing process improvement

Improvement in meeting security and resiliency goals is dependent on active management of the process

Process maturity increases capability for meeting goals and sustaining the process

“Are we secure?” is answered in the context of capability, not threat or incident – success more predictable, controllable?

Meaningful, purposeful selection of practices

Capability areas

Capabilities cover the five resiliency objects.

Capabilities traverse many organizational entities and functions.

- Enterprise
- People
- Technology assets and infrastructure
- Information and data
- Physical plant
- Resiliency relationships
- Resiliency delivery
- Sustaining resiliency

*To date, we have identified 42 candidate capabilities.

A maturity model?

Potential barriers of maturity modeling for security and resiliency

“Process maturity for security” refers to competency and preparedness, *not how secure an organization is*

Need to explore maturity model structures for defining security and resiliency processes

Must consider connection to CMMI, other models

What are we doing?

A framework for security and operational resiliency

- Describes a set of enterprise capabilities that collectively define the process
- Defines a roadmap for process measurement and improvement
- Links to common practices and activities
- *Descriptive*, not prescriptive

A framework is useful to. . .

Understand the essential capabilities necessary to manage security effectively to achieve goals

Gauge current level of capability

Determine the necessary level of capability given organizational drivers

Develop a road map for process improvement to meet desired target

Improve selection and implementation of complimentary security practices to achieve goals

Improve regulatory compliance competencies

How do we get there?

Affinity grouping of standards, guidelines, practices

Developing and defining capability areas

Determining institutionalizing features—collaboration between capability areas

- “products, activities, agents”

Exploring capability and maturity modeling characteristics

Practice mapping and analysis

What do current best practices tell us?

What capabilities do they represent?

Over 750 practices representing

- COBIT
- BS7799/ISO17799
- ITIL
- ISF
- NIST 800 series
- SEI BOK
- DRII

ESM Project -1

Process improvement approach for security management

Focused on *operational resiliency* of business processes and related assets

- People
- Information
- Technology
- Facilities

Process is defined and executed at the enterprise-level

ESM Project -2

Approach instantiated in process improvement framework called PrISM

Incorporates practices/activities from three primary disciplines

- Security
- Business continuity/disaster recovery
- IT operations and service delivery disciplines

Describes the “resiliency engineering” process

ESM Project -3

Covers processes in four areas

- Enterprise
- Operations
- Engineering
- Process Management

PrISM Framework -1

Describes process for managing the resiliency engineering process

Content gathered from CERT field experience, data collection from high-performing organizations, and existing practice sources

Structured like CMMI: specific goals, practices, and sub-practices

No current maturity structure

PrISM Framework -2

Sub-practices are seeded from and cross-referenced to common bodies of practice

- CobiT (IT)
- ITIL (IT/Security)
- BS7799 (Security)
- DRII GAP (Business Continuity)

Currently developing v1.0 for release September 2006

PrISM Framework -3

Sample Process Areas

- Requirements Development
- Requirements Management
- Asset Management
- Supplier Agreement Management
- Supplier Relationship Management
- Access Management
- User Management
- Continuity Planning
- Event Identification and Analysis

Collaborating with industry -1

Recent collaboration with Financial Services Technology Consortium

Advancing concepts of resiliency and security process management through the financial services industry

Completed phase I data collection and analysis

“Resiliency Model” project

More information: www.fstc.org

Collaborating with industry -2

Ameriprise Financial

Bank of America

Capital Group

Citigroup

Discover Financial

DRII

Federal Reserve Bank NY

IBM

Interisle Consulting

IBM

JPMorganChase

Key Bank

KPMG

Marshall & Ilsley

Mastercard

SunGuard

USBank

Wachovia

Why are they interested?

Role in U. S. and world economies

Complexity of operations and interdependencies

Need to control “resiliency value chain”

Regulatory environment

Need to drive down cost and improve value

Build on process improvement analogs

Future considerations

Questionnaire to benchmark financial and banking industry against current framework

Exploration of process maturity concepts

Exposure to process community (quicker to understand model and approach)

Ability to explain overlap with CMMI to process audience/users

Utilize existing SEI structure/expertise to promote

FSTC phase II objectives

Evolution of process improvement concepts (technical note, March 2006)

Completion of v1.0 of framework (technical note planned for September 2006)

Development of normalized taxonomy

Deployment of practices questionnaire

Identification of process improvement metrics

Getting involved

Opportunities for

- Collaborative development
- Framework review and commenting
- Pilot use of framework

For more information

Technical Notes:

- “Managing for Enterprise Security” (12/2004)
- “Sustaining Operational Resiliency: A Process Improvement Approach to Security Management” (3/2006)
- Framework introduction v1.0 (9/2006)

Web:

- www.cert.org (Green Portal-ESM)
- www.fstc.org