CERT

Homeland Security

A Process Approach to Management of Operational Cyber Security Risks

DOE Cyber Security Conference
Atlanta – May 2010

Antione Manson, DHS
Jim Cebula, CERT

NO WARRANTY

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE IS FURNISHED ON AN “AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this presentation is not intended in any way to infringe on the rights of the trademark holder.

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.

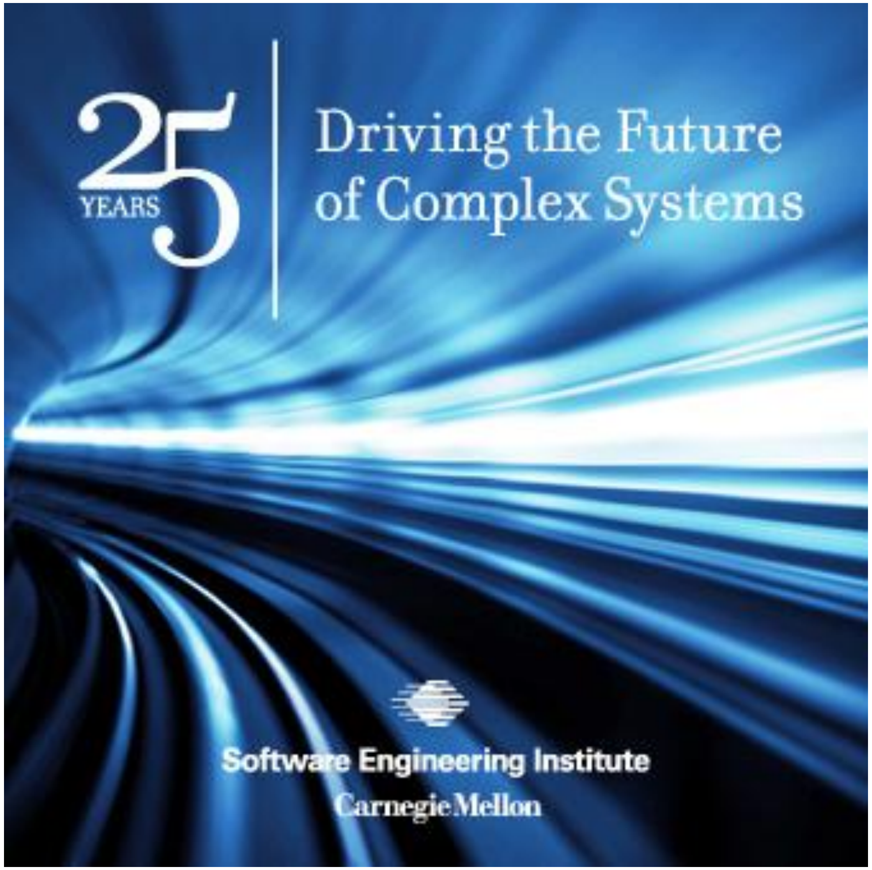
Why are we here?

Homeland Security

- DHS National Cyber Security Division, Federal Network Security has responsibility to assess the cyber risk posture across the Federal Civilian Agency (FCA) space.
- DHS-FNS engaged with SEI-CERT to develop tools and methods to accomplish this.
- DOE/NNSA has partnered with us in an early trial of the method.

What is CERT?

- Located in the Software Engineering Institute (SEI)
  - A Federally Funded Research & Development Center (FFRDC)
  - Operated by Carnegie Mellon University (Pittsburgh, Pennsylvania)
- Established in 1988 by the US Department of Defense in response to the Morris worm
- Main areas of work
  - Software Assurance
  - Secure Systems
  - Organizational Security
  - Coordinated Response
  - Education and Training


25 YEARS
Driving the Future of Complex Systems
Software Engineering Institute
Carnegie Mellon

Welcome – What we'll discuss

- Operational risk and resilience
- Assets defined
- Relationships among services, business processes, and assets
- Protection and sustainability
- The need for a process approach
- The DHS Federated Cyber Resilience Management Program (Fed-CRMP)
- DHS FNS Pilot activities
- Future work

Operational Risk and Resilience

Risk defined

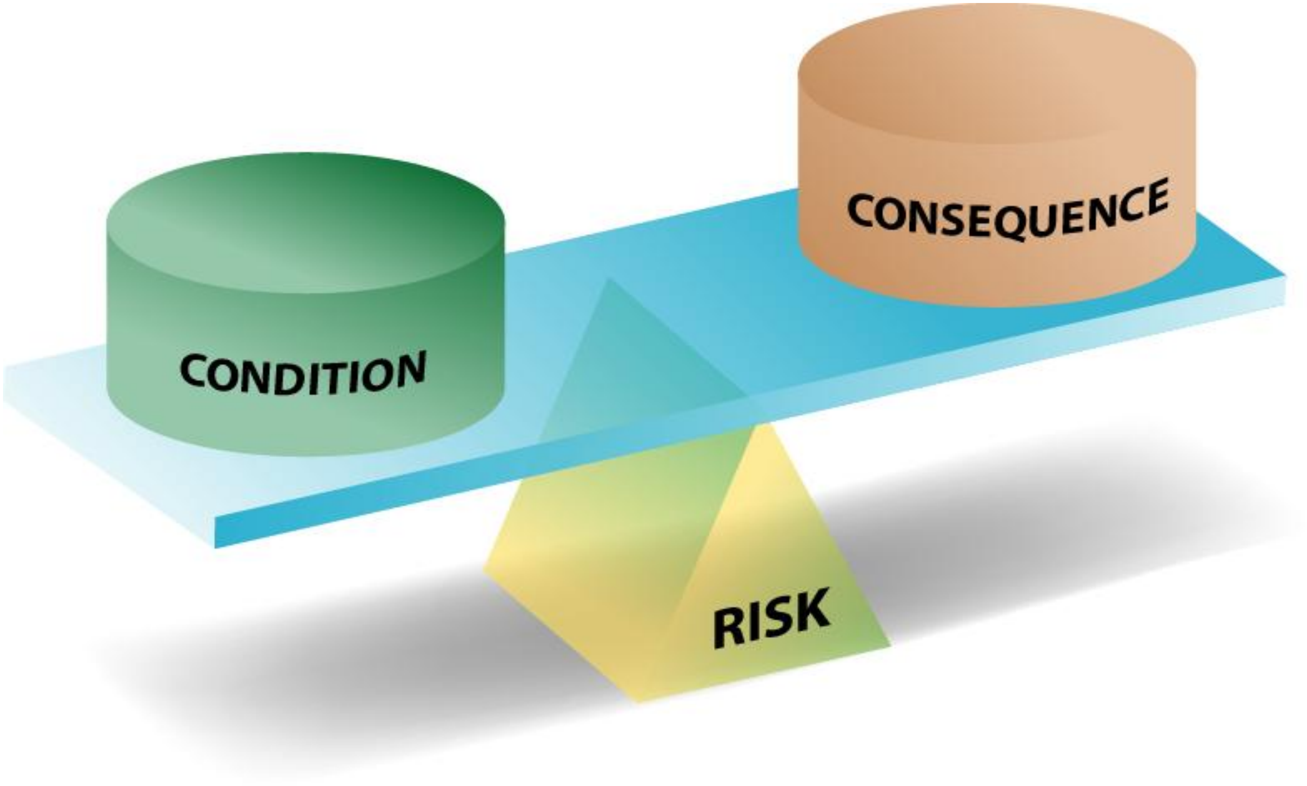
The possibility of suffering harm or loss

Hazard; a source of danger; a possibility of incurring loss or misfortune [wordnet.princeton.edu]

Risk consists of

- An event or condition
- A consequence or impact from the condition
- Uncertainty

The basic risk equation



Operational risk

A form of hazard risk affecting day-to-day business operations

The potential failure to achieve mission objectives

Typically categorized as follows:

Actions of people

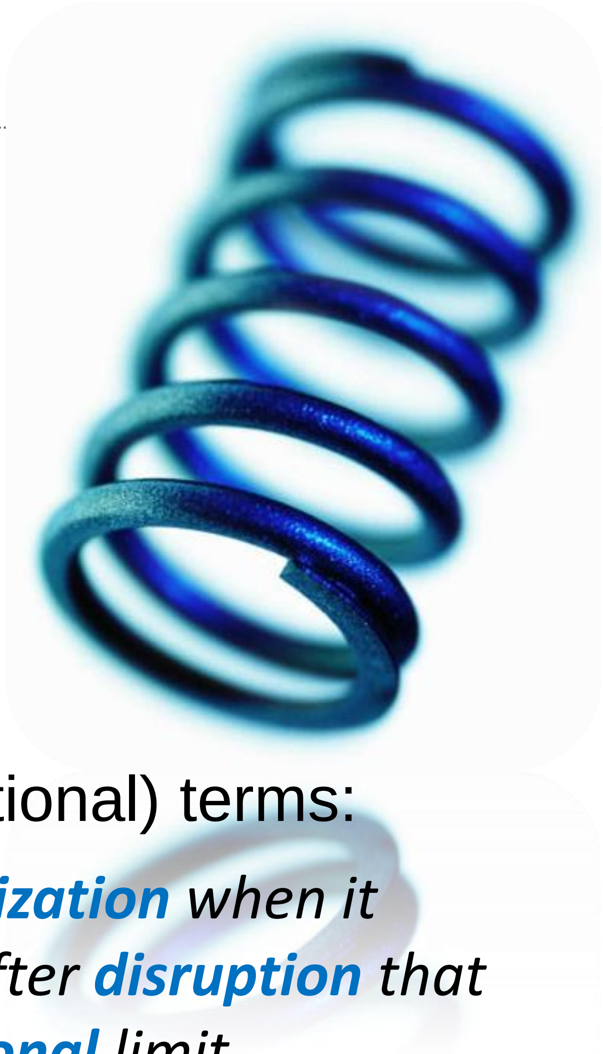
```
A fatal exception
000059F8. The curr

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

Systems & technology failures

Failed internal processes

External events

Resilience 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*

Challenges for the organization

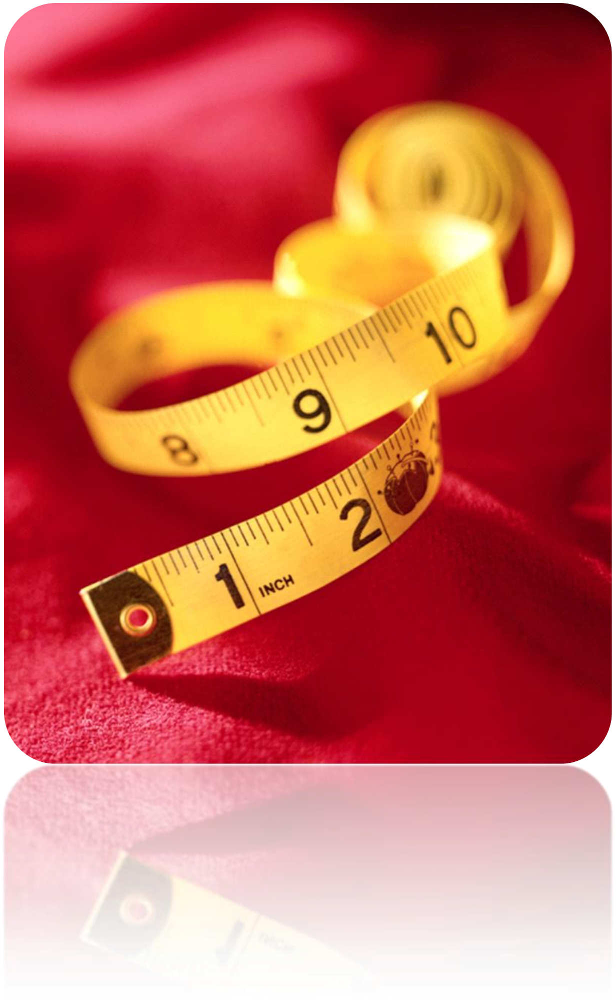
Meet mission ***no-matter-what***

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



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 risk management activities are deployed toward the same objectives
- work related to managing operational resiliency is planned, executed, managed, measured, and improved

The principle of 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
- I/T operations and service delivery management

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

Assets

Assets

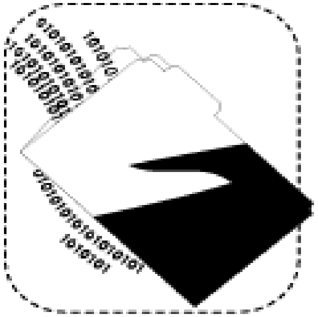
Something of value to the organization

“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.

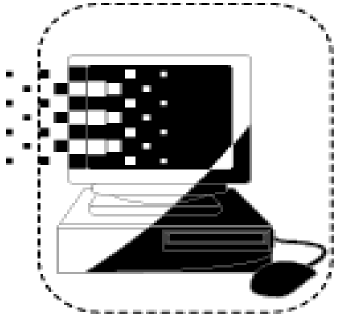
Assets

people



information

facilities

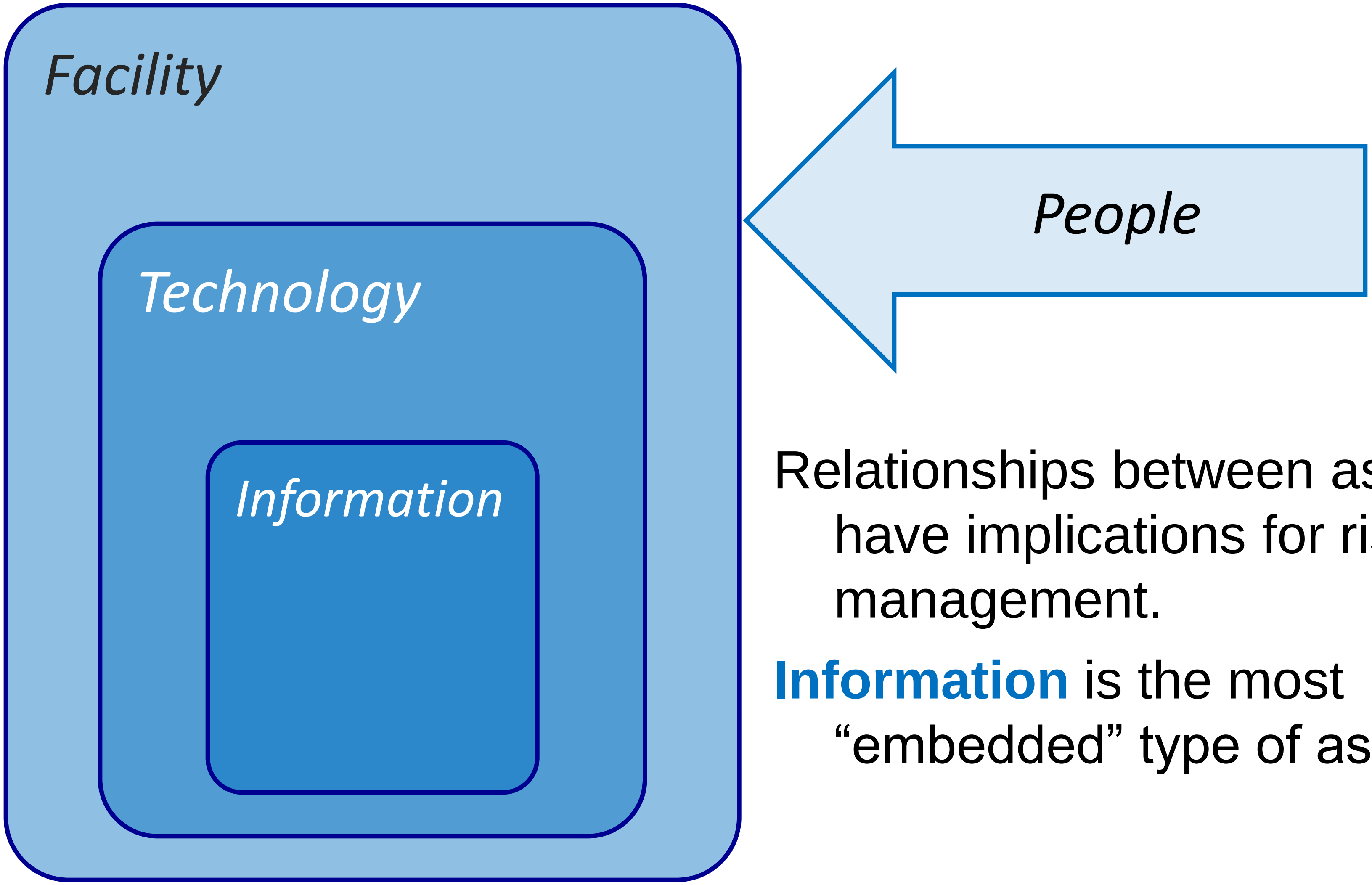


technology

Four types of assets are considered in operational risk management. These include **people, information, facilities, and technology.**

Management of *operational cyber security risks* is directly focused on information and technology assets. People and facility assets are considered to the extent that they support information and technology.

Putting assets in context

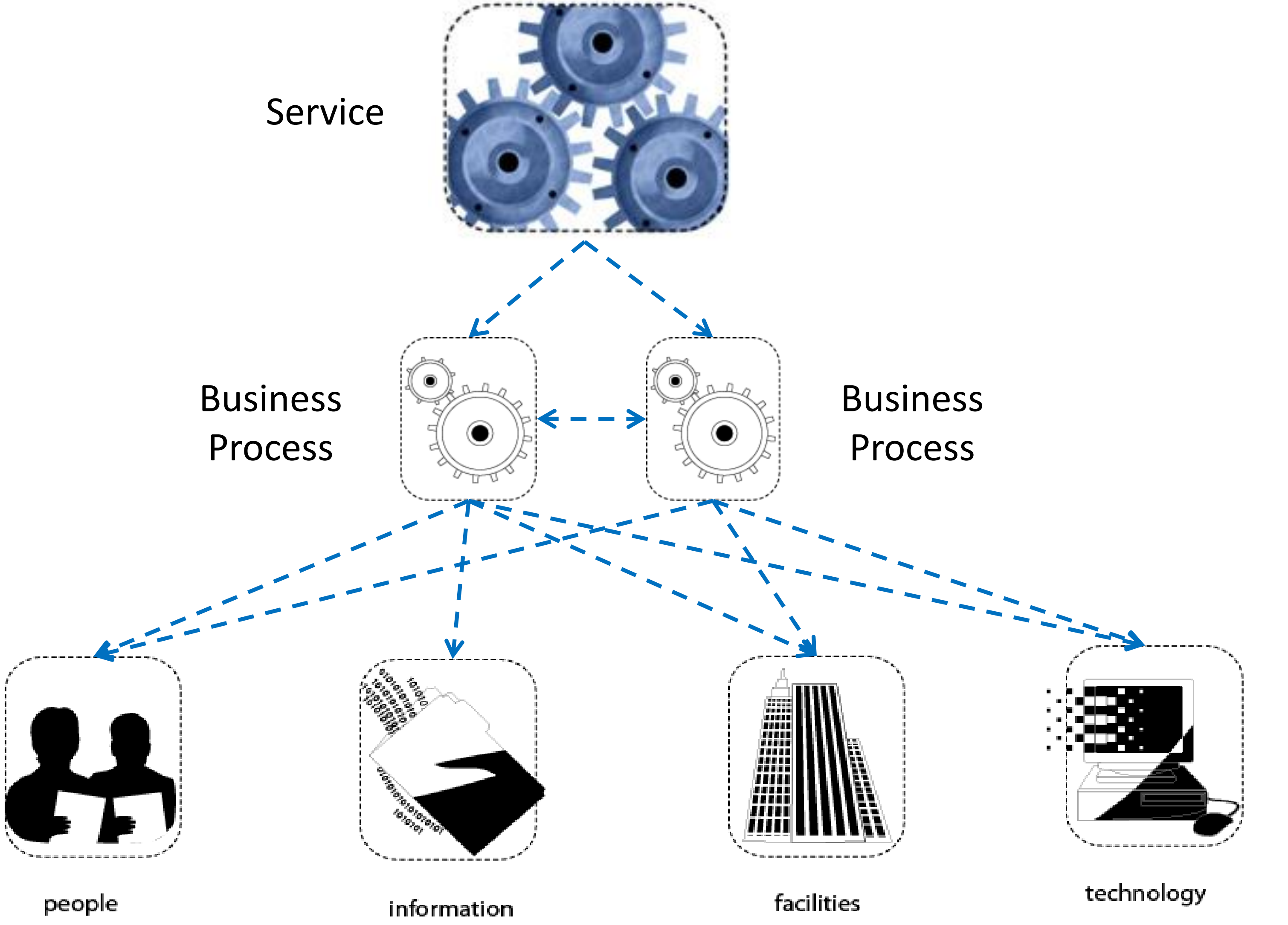


Relationships between assets have implications for risk management.

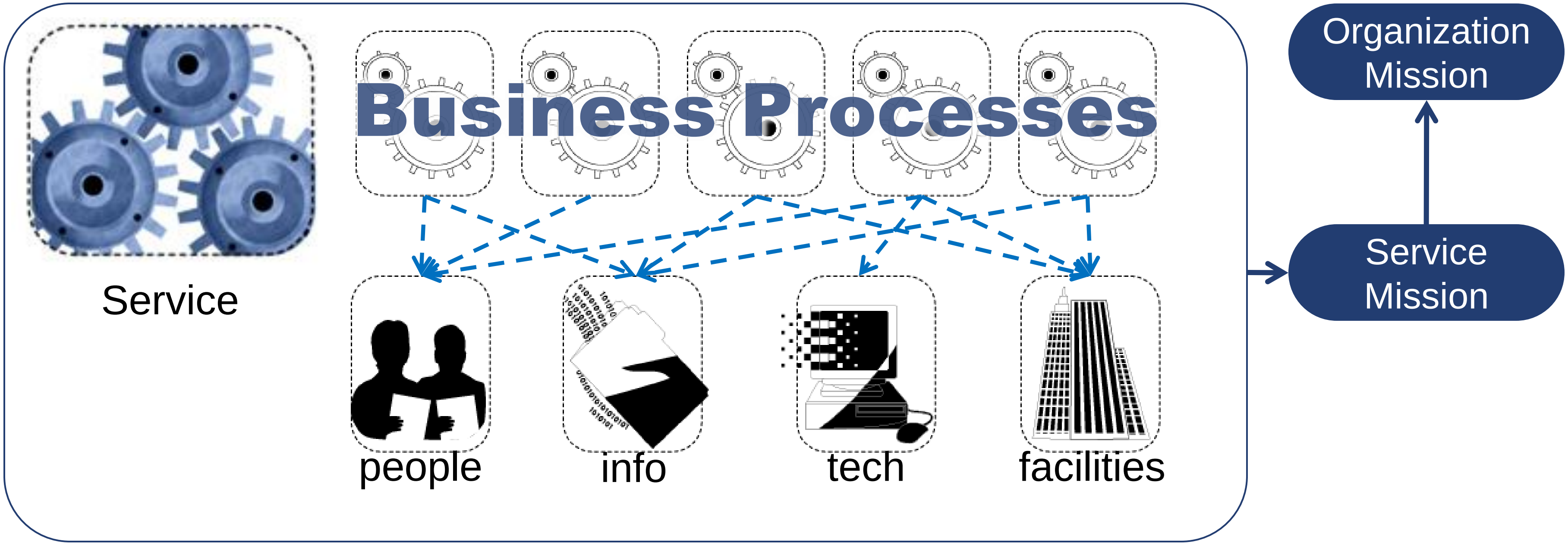
Information is the most "embedded" type of asset.

Relationships of Assets, Business Processes, and Services

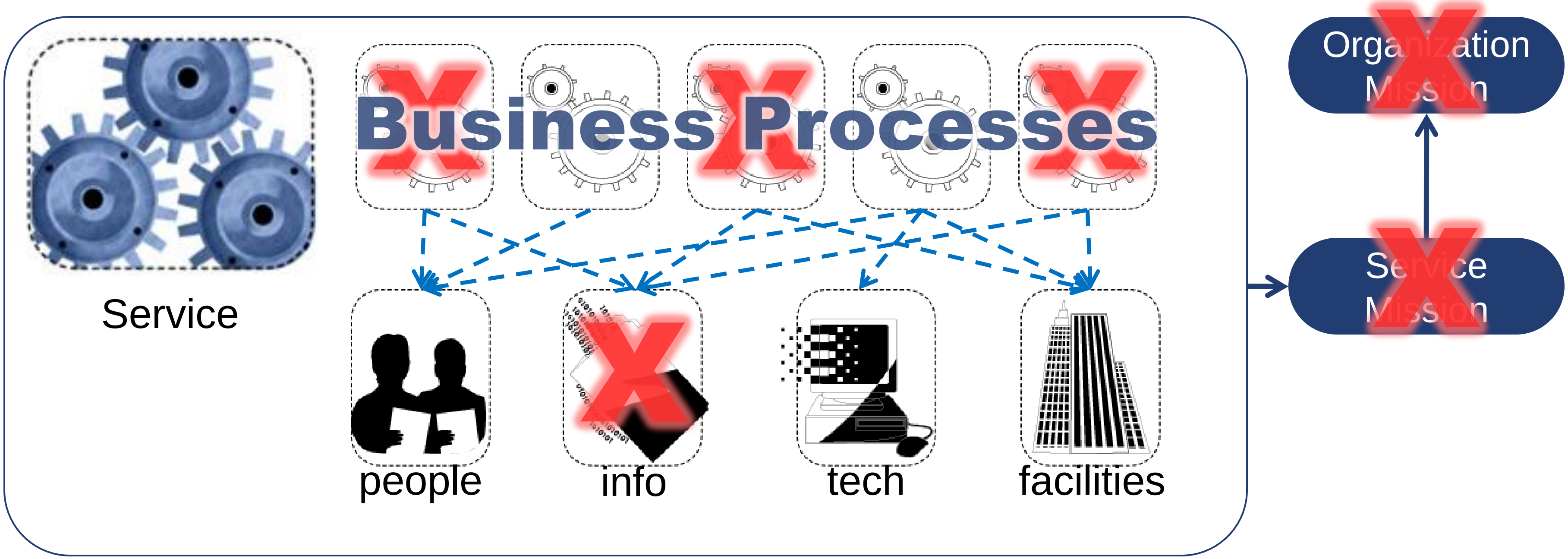
Relationships between elements



Abstracting to a mission focus



Impact of disrupted asset on service mission



The failure of one or more assets has a cascading impact on the mission of related **business processes**, **services**, and the **organization** as a whole.

Protection and Sustainability

Protection and sustainability

The strategies developed to identify, develop, implement, and manage controls commensurate with an asset's resiliency requirements

Protection strategies are protective—address how to minimize the asset from exposure to threats and vulnerabilities.

Sustainability strategies are continuity-focused—address how to

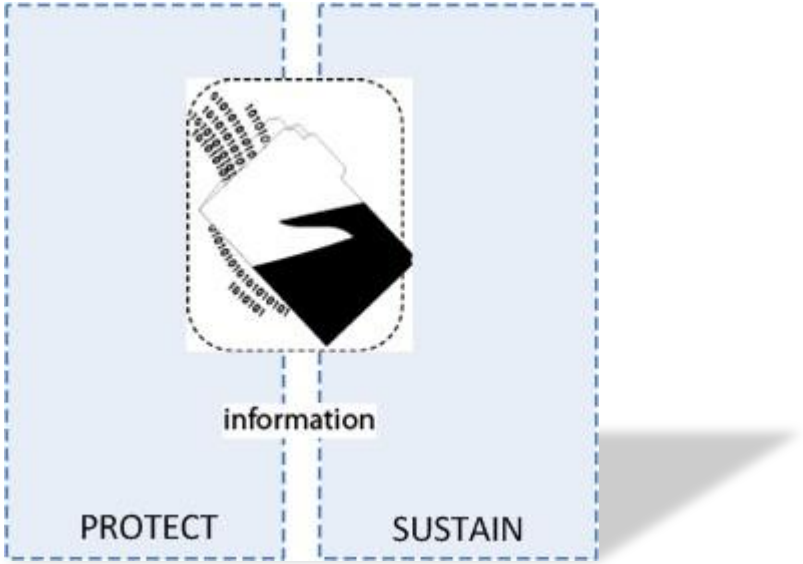
- keep the asset operable when adversely affected or
- how to keep an associated business process or service operable without the asset's contribution

Each asset needs an optimal balance of these strategies.

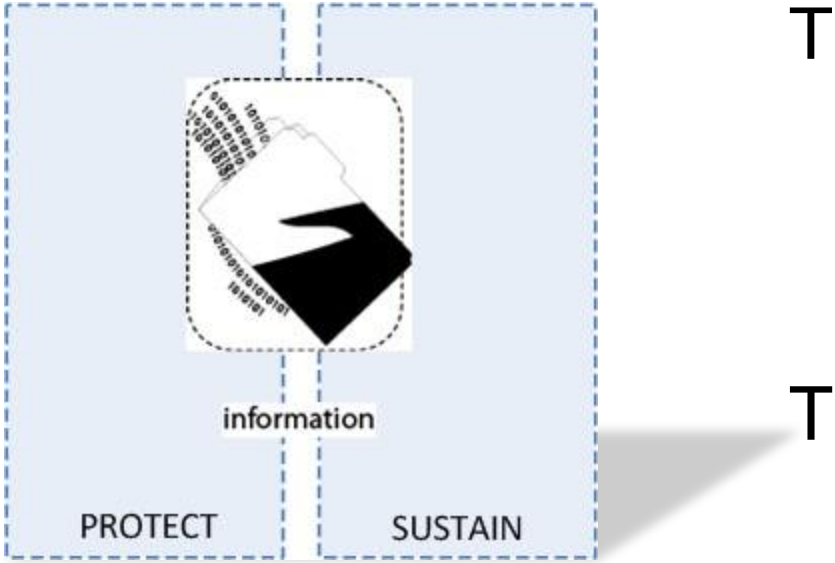
Protection strategies

Translate into activities designed to keep assets from exposure to disruption

Typically “security” or “controls” activities, but may also be imbedded in IT operations activities



Sustainability strategies

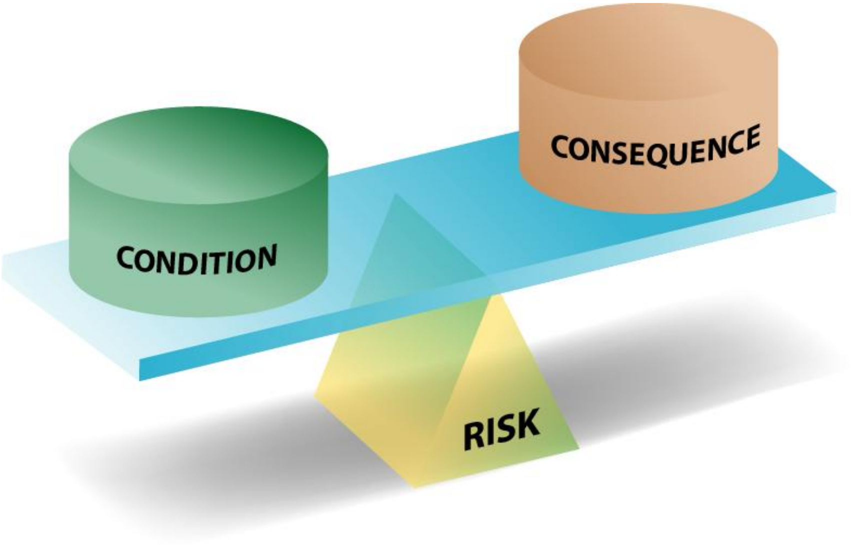


Translate into activities designed to keep assets productive during adversity

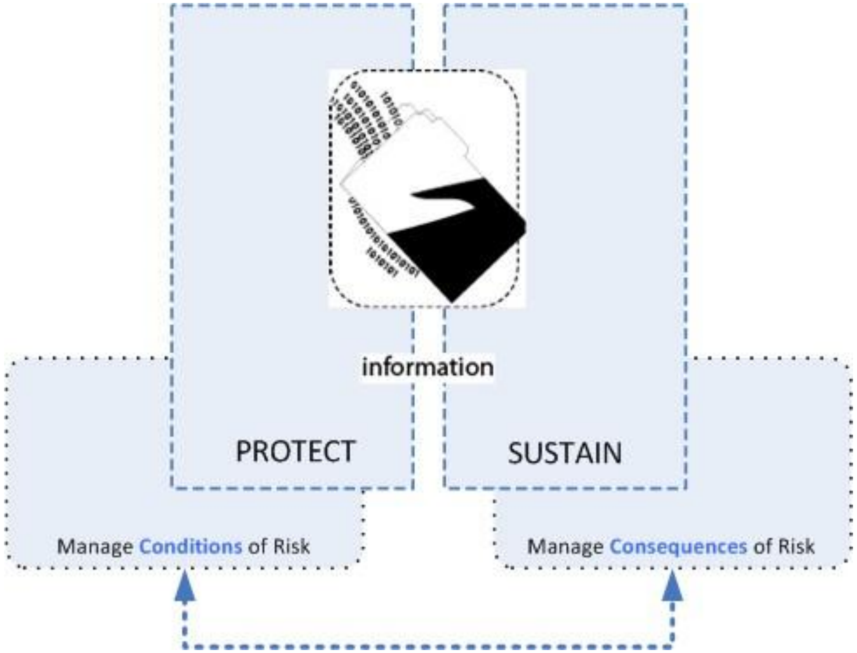
Typically “business continuity” activities

Protection, sustainability, and risk

Basic risk equation



Protection & sustainability



The Need for a Process Approach

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

National Institute of Standards and Technology NIST

...working with industry to foster innovation, trade, security and jobs

Protect Patient Information

PCI Security Standards Council™

PARTICIPATING ORGANIZATION

ISO International Organization for Standardization

DEFENSE INFORMATION SYSTEMS AGENCY

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.

Developing a solution

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

1. The ability to define the **range of activities** required to manage operational risks (both practices and process)
2. The ability to *measure* the degree to which an organization has the process maturity to **sustain their managerial capabilities - ** Remember resilience is a property. It is difficult to directly measure the quality of a property. We instead need to measure the quality of the process.

Doing vs. managing

Most organizations have experience at the tactical level

- Significant body of **codes of practices** to guide effort
- Significant range of **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 (in the steady state)
  - under times of stress
  - under uncertain conditions
  - when the risk environment changes

Technology-centric approaches

Fail to recognize that managing operational risk is an organizational problem

Can be ineffective if they are not actively managed and continuously improved

Often leave management to ask: “If we have state-of-the-art technologies deployed, why do we still suffer disruptions?”

Move past “vulnerabilities”

Vulnerability assessment is NOT risk assessment

Vulnerability assessment is for identifying “conditions”

Conditions must be taken in the context of the organization’s unique operating circumstances

There must be a consideration of “consequence” to be meaningful

Move past “controls”

Heard at this conference …

“The solution is broader than a control catalog”

“Sites are having trouble with ‘Risk Management’ that is controls based since that leads to a compliance mindset.”

“The controls and system security activities must be related to a business impact analysis.”

Moving toward process effectiveness

FY 2010 FISMA Reporting per **OMB M-10-15** is starting agencies in that direction:

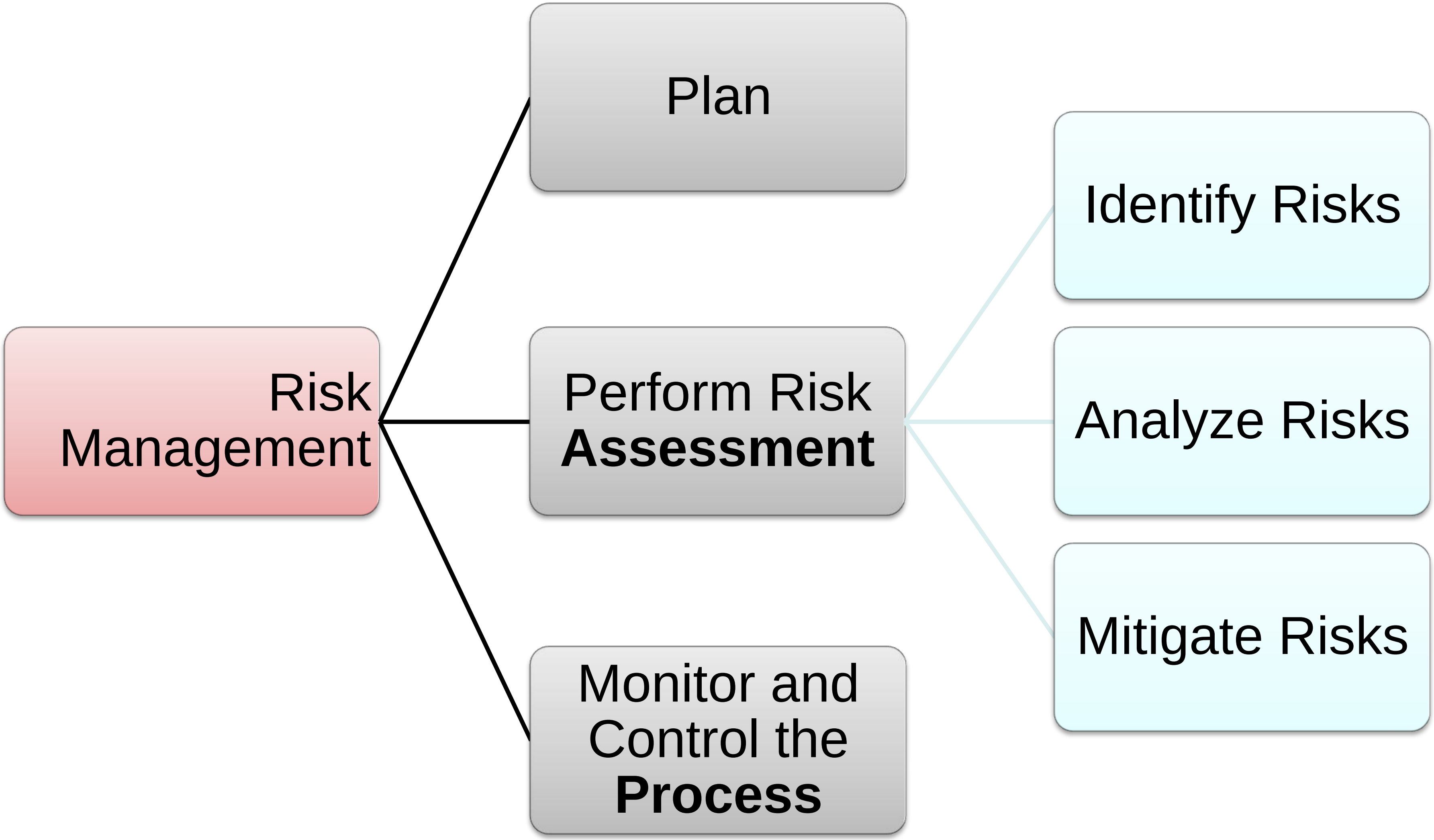
- Data Feeds from Security Management Tools - *Security State Information*
- Government-wide Benchmarking on Security Posture – *Practice Implementation*
- Agency Specific Interviews – *Starting the discussion with agencies regarding impact of cyber risks to their mission, along with their risk management process capability*

Enterprise Perspective

An enterprise view of operational risk management

- Enables risk mitigation decisions that effectively deploy limited resources
- Integrates with enterprise architecture approaches to security management
- Supports NIST SP 800-39’s “Risk Executive” function
- Incorporates physical and cyber security management

Risk Management vs. Risk Assessment



Risk Management

Plan

Perform Risk **Assessment**

Monitor and Control the **Process**

Identify Risks

Analyze Risks

Mitigate Risks

The DHS Federated Cyber Riesilience Management Program (Fed-CRMP)

Federated Cyber Resilience Management Program (Fed-CRMP)

- Being developed by SEI-CERT for DHS-FNS
- Built from published CERT bodies of work
  - Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) method
  - Resilience Management Model (RMM) – 26 process areas
- Tools being developed to support the Program
  - Risk Taxonomy (Common description of risks)
  - Diagnostic Assessment Instrument (Question based)
  - Process Measurements
    - Implementation (are you doing something)
    - Process Performance (how are you doing it)
    - Efficacy/Effectiveness (is it working)

Fed-CRMP Assessment Questions

The question based process provides a consistent way to perform an assessment across the Federal Civilian Agency space.

The questions ask about practices and existence of risk across all four categories (people, technology, process, external events)

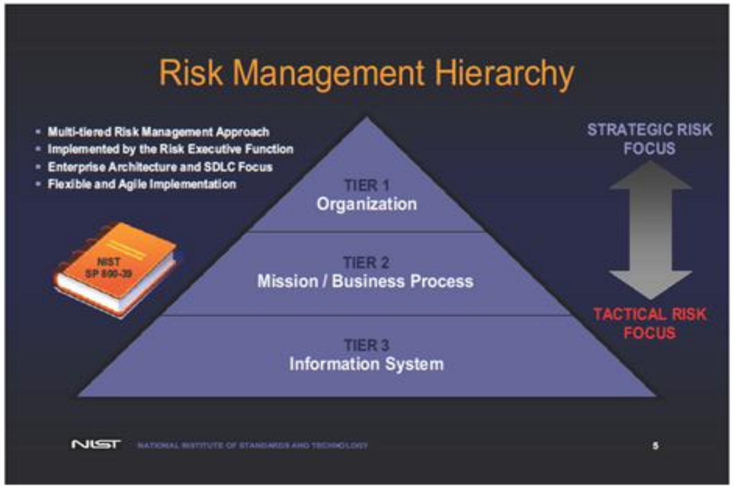
- “High” scores will give an indication of an organization’s ability to both perform a practice and have a process to repeat that performance, but do not equate to maturity levels.

When asked to a sufficiently large number of organizations, the answers to the questions can be used to establish a performance baseline.

Relationship to NIST Guidance

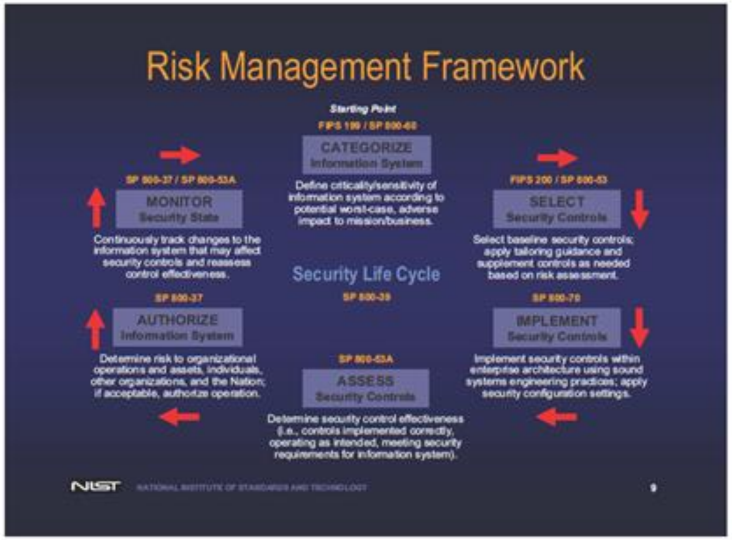
- NIST provides *guidance*
  - Risk Hierarchy forms the basis for an enterprise risk management program (800-39)
  - Risk Management Framework addresses controls management (800-37, 800-53, *et. al.)*
- Fed-CRMP maps to a *risk ecosystem* to actualize and extend the NIST guidance

http://scap.nist.gov/events/2009/itsac/presentations/day3/Day3_General_Ross.pdf



Risk Management Hierarchy

- Multi-tiered Risk Management Approach
- Implemented by the Risk Executive Function
- Enterprise Architecture and SDLC Focus
- Flexible and Agile Implementation



Risk Management Framework

Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.

Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

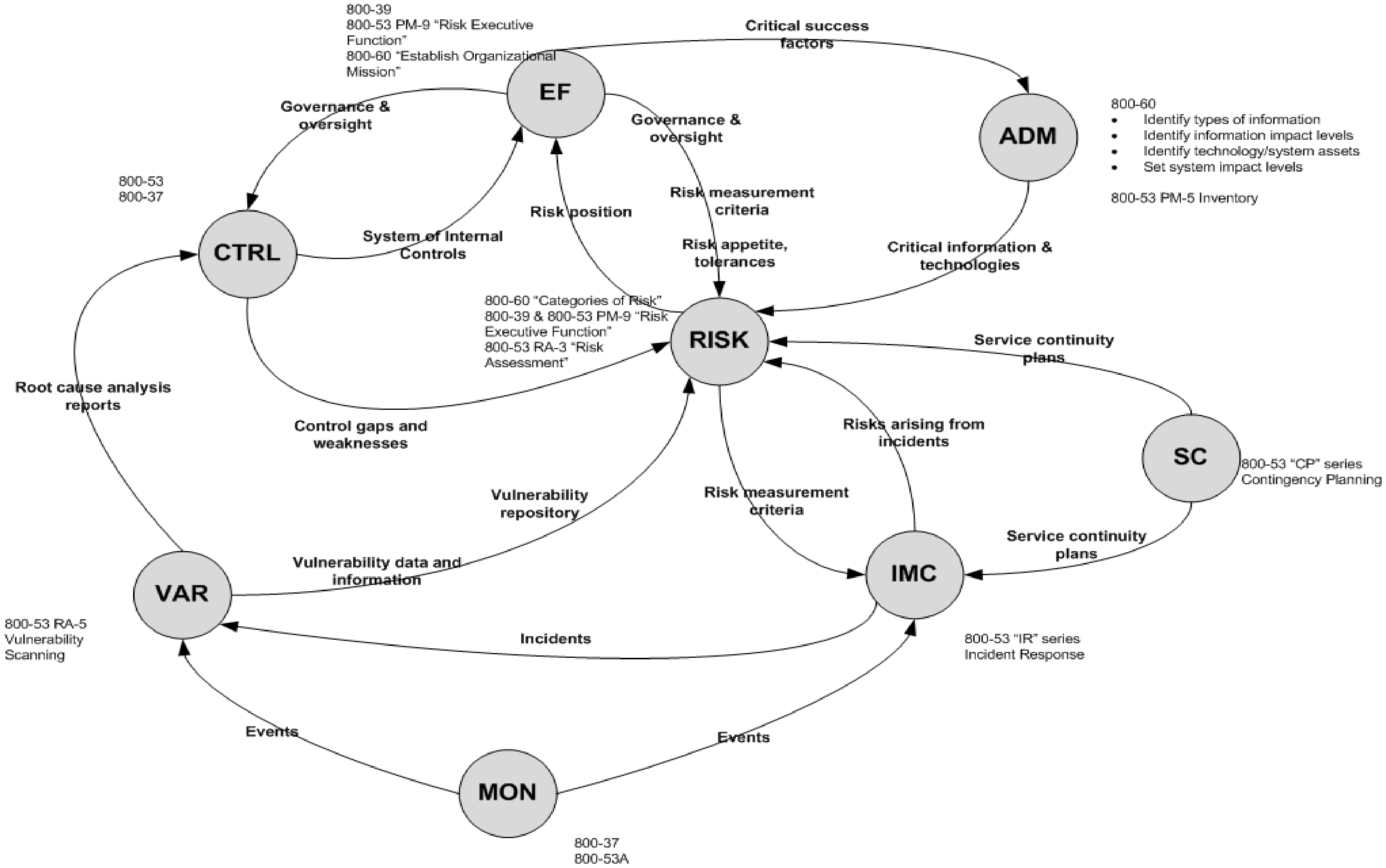
Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

Continuously track changes to the information system that may affect security controls and reassess control effectiveness.

Fed-CRMP 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)

Risk Ecosystem example



EF
ADM
CTRL
RISK
SC
IMC
VAR
MON
Critical success factors
Governance & oversight
Governance & oversight
System of Internal Controls
Risk position
Risk measurement criteria
Risk appetite, tolerances
Critical information & technologies
Service continuity plans
Root cause analysis reports
Control gaps and weaknesses
Risks arising from incidents
Vulnerability repository
Risk measurement criteria
Service continuity plans
Vulnerability data and information
Incidents
Events
Events

800-39
800-53 PM-9 "Risk Executive Function"
800-60 "Establish Organizational Mission"

800-60
- Identify types of information
- Identify information impact levels
- Identify technology/system assets
- Set system impact levels

800-53 PM-5 Inventory

800-53
800-37

800-60 "Categories of Risk"
800-39 & 800-53 PM-9 "Risk Executive Function"
800-53 RA-3 "Risk Assessment"

800-53 "CP" series
Contingency Planning

800-53 RA-5
Vulnerability Scanning

800-53 "IR" series
Incident Response

800-37
800-53A

Alignment with NIST Risk Management Framework

Fed-CRMP

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, link assets to services, and provide an enterprise view)

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 a solid foundation for a controls management program based on control selection

Identifies classic threats and vulnerabilities

Integration with Other Programs

NIST Risk Management Hierarchy

- DHS and SEI/CERT are collaborating with NIST to align with the upcoming revision to 800-39.

Other DHS Programs

- SEI/CERT partners with DHS across a range of programs and initiatives. Fed-CRMP is designed to be complementary to these other initiatives:
  - Trusted Internet Connection (TIC)
  - OMB/FISMA reporting
  - Critical Infrastructure Protection

DHS FNS Pilot Activities and Future Work

Purpose & Outcome of Fed-CRMP pilot

Purpose: Develop a Federated Cyber Risk Management Program (Fed-CRMP) approach to characterize the cyber-readiness of civilian agencies across the enterprise to:

- Provide agencies with techniques and methods to enhance cyber security posture by assessing both practices and processes.
- Capture data during the pilot and refine the method.
- Develop an initial view of the enterprise risk landscape across the federal civilian agency space.

Desired Outcomes: Pilot the Fed-CRMP techniques and methods to understand the as-is capability to manage risk across the federal government and use this information to drive improvements in cyber readiness and resilience.

DOE Pilot Activities

- DHS briefed NNSA OCIO in March 2010
- Follow-up briefing provided to NNSA site leadership in April 2010
- Currently starting up pilot with NNSA-HQ
  - Scheduling initial diagnostic assessment
  - This will be an iterative process
  - Possible expansion to other NNSA sites
- In parallel, several other agencies have expressed interest in starting pilots

Who is conducting the pilot?

DHS Federal Network Security is sponsoring and conducting the pilot with support from SEI/CERT.

Activities include:

- Conduct benchmarking assessments to understand current cyber security operational capabilities
- Use benchmarking results to assess gaps in current capabilities to manage operational cyber security risks.
- Analyze gaps to inform cyber risk decision making and priorities.
- Mature processes over time to increase cyber capabilities.

Future Work

- Utilize information learned in the pilots to refine the product suite:
  - Refine the assessment instrument
  - Further develop the process measurements
- Build a common view of resilience across the Agencies for DHS
- Conduct second round of pilots
- Provide risk management training/workshops

Contacts

DHS

Antione Manson

antione.manson@dhs.gov

703-235-5228

SEI-CERT

www.cert.org/resilience

Jim Cebula	Lisa Young
jcebula@cert.org	lry@cert.org