



Resiliency Engineering Framework

Project Update

David White – SEI

Charles Wallen - FSTC

FSTC Annual Meeting

11 October 2006



Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE 11 OCT 2006		2. REPORT TYPE		3. DATES COVERED 00-00-2006 to 00-00-2006	
4. TITLE AND SUBTITLE Resiliency Engineering Framework: Project Update				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Carnegie Mellon University ,Software Engineering Institute (SEI),Pittsburgh,PA,15213				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

The Resiliency Model Project

Collaboration between FSTC and Carnegie Mellon's Software Engineering Institute

Multi-phased effort to help financial organizations to measure and improve their resiliency capabilities

Focused on the resiliency engineering process

Encompasses security, business continuity, and IT operations practices with focus on operational risk management

Codified in the "Resiliency Engineering Framework"

Establishes a foundation for resiliency process improvement

Software Engineering Institute

Established in 1984

Federally Funded Research and Development Center (FFRDC)

College-level unit of Carnegie Mellon University

Includes five technical programs aimed helping defense, government, industry, and academic organizations to continually improve software-intensive systems

Widely-known areas of expertise

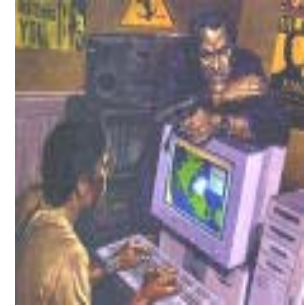
- CERT Coordination Center (security)
- CMMI Capability Maturity Model Integration (process improvement)



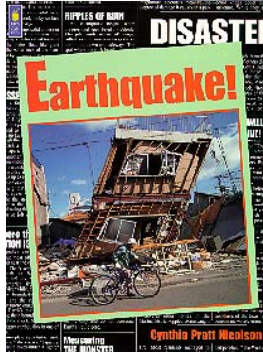
An expanded risk environment



Regulations



Cyber Security



Disasters

Supply Chain



Infrastructure



Terrorism



Resiliency...more than a buzzword

Resiliency is the ability of an object to return to its original shape

Operational resiliency refers to an organization's ability to function and adapt through the lifecycle of disruptions

A resiliency model is a roadmap for managing the consistent delivery of products and services



Managing resiliency is a challenge

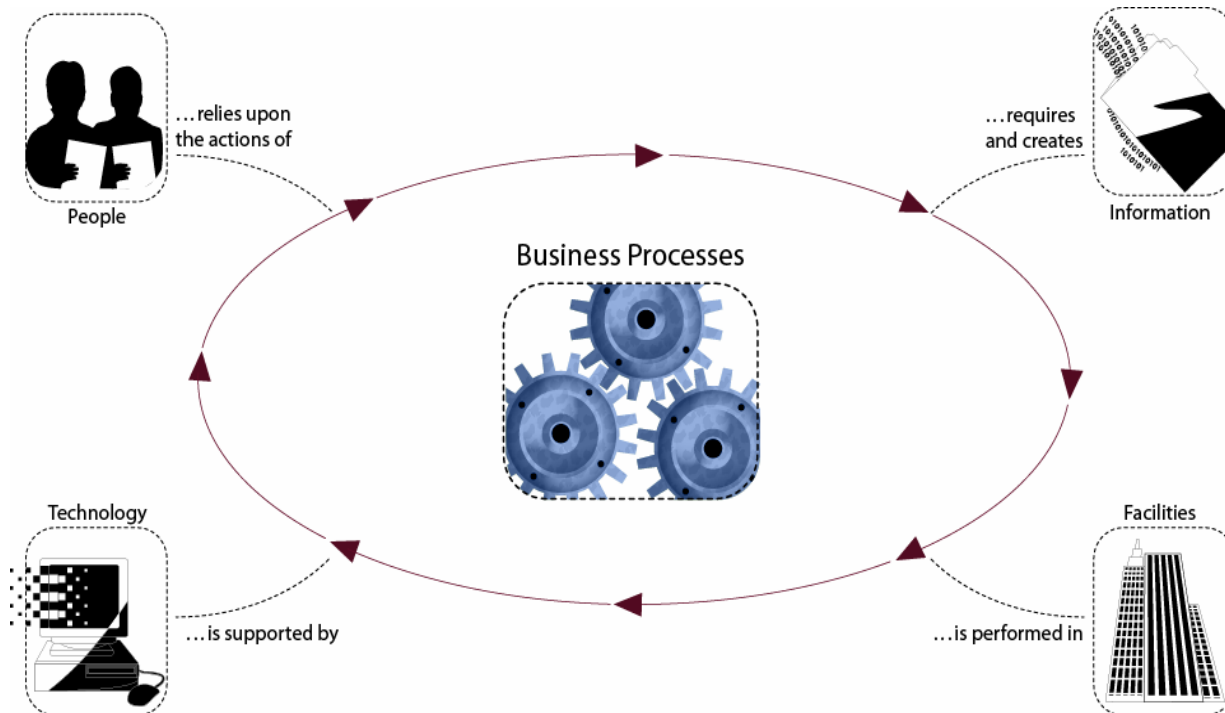
Requires

- Ongoing measurement and monitoring
- Balancing cost and risk tradeoffs
- Taking an enterprise focus

Financial Services organizations recognize a need to be able to manage resiliency in a systematic, consistent, measurable, and improvable way



Resiliency engineering in practice



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

Collaborating toward a common goal



A framework is needed to. . .



Identify and prioritize risk exposures

Define a process improvement roadmap

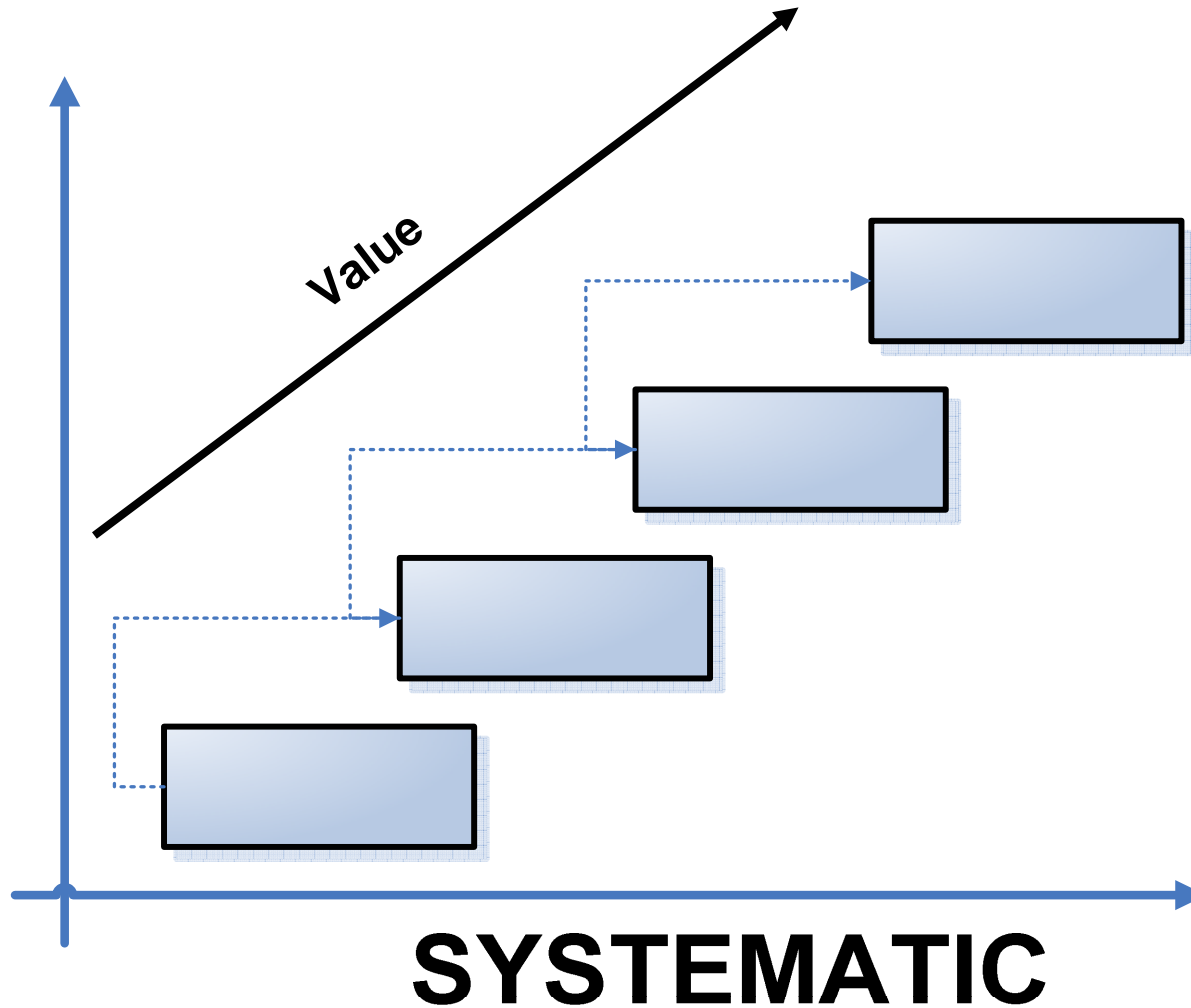
Measure and facilitate strategic planning

Address interdependencies

Promote pro-active regulatory compliance



Goal: continuous improvement of resiliency processes



Why use a “framework” approach?

- Provides an operational risk roadmap
- Vendor-neutral, standardized, unbiased assessment vehicle
- Can be leveraged for process improvement at any organization, public or private
- Avoids the pitfalls of prescriptive solutions by promoting resiliency engineering and the use of organization-appropriate practices



The Resiliency Engineering Framework

An integrated process improvement framework for security and business continuity

Defines basic process areas and provides guidelines for improving security and BC processes

Addresses operational risk management through process management

Vital linkages between security, BC, and I/T ops are captured in the process definition

Establishes a capability benchmark

Why use a “process” approach?

Elevates the management and coordination of operational-resiliency focused activities to the enterprise:

- Shared view of risk, goals, and resources
- Elimination of redundancy and stovepipes
- Elimination of “practice quagmire” by selecting meaningful practices that fit the process definition
- Ability to set goals and measure process effectiveness
- Ability to inculcate and nurture a process improvement culture

How will the framework be used?

Establish current level of capability

Set forward-looking resiliency goals and targets

Develop plans to close identified gaps

Build resiliency into important assets and architectures

Reduce reactionary activities; shift to directing and controlling activities

Align common practices with processes to achieve process goals

Future activities

Release REF v1.0 in October 2006 for comments

Guidelines for improving the security and business continuity processes

Phase III expansion of model development and piloting

Exploration of integration with other existing models

Development of appraisal methodology to measure capability for managing resiliency

Phase I and Phase II Project Members

Ameriprise

Bank of America

Carnegie Mellon

Capital Group

Citicorp

Discover

DRII

DRJ

IBM

JPMorgan Chase

Key Bank

KPMG

MasterCard

Marshall and Ilsley

NY Federal Reserve Bank

SunGard

Trizec Properties

US Bank

Wachovia

For more information



Rich Caralli

Software Engineering
Institute

www.sei.cmu.edu

www.cert.org

rcaralli@cert.org



Charles Wallen

Financial Services
Technology Consortium

www.fstc.org

charles.wallen@fstc.org



Introducing the Resiliency Engineering Framework



Software Engineering Institute

Carnegie Mellon



© 2006 Carnegie Mellon University

Framework architecture

Represents processes that span four basic areas:

- Enterprise management
- Engineering
- Operations management
- Process management

Considers the resiliency of people, information, technology, and facilities in the context of services and business objectives

Enterprise management processes

Enterprise capabilities that are essential to supporting the resiliency engineering process

RISK – Risk Management

EF – Enterprise Focus

COMP – Compliance Management

FRM – Financial Resource Management

HRM – Human Resource Management

Operations management processes

Capabilities focused on sustaining an adequate level of operational resiliency

SAM – Supplier Agreement Management

SRM – Supplier Relationship Management

AMC – Access Management and Control

IMC – Incident Management and Control

VM – Vulnerability Management

EC – Environmental Control

KIM – Knowledge and Information Management

SOM – Security Operations Management

ITOPS – IT Operations Management

TM – Technology Management

Engineering processes

Capabilities focused on establishing and implementing resiliency for organizational assets, business processes, and services

RRD – Requirements Definition

RRM – Requirements Management

ADM – Asset Definition and Management

SM – Survivability Management

REST – Restoration of Operations Planning

CM – Controls Management

RADA – Resilient Architecture Development and Acquisition

Process management processes

Enterprise capabilities related to defining, planning, deploying, implementing, monitoring, controlling, appraising, measuring, and improving processes

OTA – Organizational Training and Awareness

PM – Process Management

MA – Measurement and Analysis

MON - Monitoring