CERT Resiliency Engineering Framework

David White
01 March 2007
Software Engineering Institute

Established 1984

Federally Funded R&D Center (FFRDC)

College-level unit of Carnegie Mellon University

Five technical programs help organizations improve software-intensive systems

Widely-known “brands”
  • CERT Coordination Center
  • Capability Maturity Model Integration (CMMI)
Agenda

Context and problem

Resiliency Engineering

Process Improvement

The CERT Resiliency Engineering Framework

Future Plans and Summary
## Today’s operational environment

<table>
<thead>
<tr>
<th>No operational boundaries</th>
<th>Increasing regulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pervasive &amp; rapidly changing technology</td>
<td>Criticality of data and information</td>
</tr>
<tr>
<td>Dynamic &amp; expanding risks</td>
<td>Distributed workforce</td>
</tr>
<tr>
<td>Fewer resources, more demands</td>
<td>Heightened threat level and increasing uncertainty</td>
</tr>
<tr>
<td>Dependency on third-parties</td>
<td>Shorter-lived skills</td>
</tr>
</tbody>
</table>

*A new environment in which business continuity & security must be increasingly effective & efficient*
## Operational risk management problems

<table>
<thead>
<tr>
<th>Poor planning and execution</th>
<th>Poorly defined and measured goals</th>
</tr>
</thead>
<tbody>
<tr>
<td>No asset management function</td>
<td>Reactive (not strategic) funding model</td>
</tr>
<tr>
<td>Seen as a technical function or responsibility</td>
<td>Compartmentalization of security and continuity activities</td>
</tr>
<tr>
<td>Searching for magic bullet: CobiT, ITIL, ISO17799, NFP1600</td>
<td>Business units not involved</td>
</tr>
</tbody>
</table>

*Many organizations are struggling with operational risk management*
Our approach

- **Resiliency Engineering**
  An integrated approach to protecting & sustaining critical business services

- **Process Improvement**
  A model-based approach to maturing enterprise capabilities

---

**CERT Resiliency Engineering Framework**
A process improvement model for resiliency engineering
Top benefits of approach

Greater efficiency of resilience activities

• Optimized resource allocation
• Appropriate and strategic investment

Objective benchmarking of resilience capabilities

• For internal improvement
• To evaluate third parties

Improved operational risk management

• Measured processes lead to measured improvement
• Better risk management yields market rewards
Resiliency Engineering:
An integrated approach to protecting & sustaining critical business services
Resiliency engineering defined

The process by which an organization designs, develops, implements, and manages the protection and sustainability of business-critical services, related business processes, and associated assets such as people, information, technology, and facilities

“Requirements-driven security and business continuity”
Resiliency engineering body of knowledge

Based on

- Affinity analysis of 750 best practices in security, business continuity, and IT operations
- Collaboration with business continuity experts from numerous US financial institutions
- Security expertise in CERT

Developed, collected, and codified over past two+ years

Forms the basis of our continuing work
Operational risk and resiliency

Operational risk is from

- Failed internal processes
- Inadvertent or deliberate actions of people
- Problems with systems and technology
- External events

Operational resiliency is the ability to sustain the mission despite these risks
A mission focus
Dependence on four critical asset types

- People
  - Relies upon the actions of
- Information
  - Requires and creates
- Technology
  - Is supported by
- Facilities
  - Is performed in
Asset focus

Resiliency emerges from effectively coordinating and managing the conditions and consequences of risk.
Achieving resiliency

Shift the paradigm

- Technical problem
- Owned by IT
- Expense-driven
- Practice-centric
- Security and BCDR
- Business problem
- Owned by organization
- Investment-driven
- Process-centric
- Enterprise resiliency

Approach resiliency as a definable, manageable, improveable, enterprise-wide process
Process Improvement:
A model-based approach to maturing enterprise capabilities
Process improvement defined

“A program of activities designed to improve the performance and maturity of the organization’s processes, and the results of such a program.”

Provides the basis for managing, sustaining, and improving the resiliency process over time

Distinguishes organizations that have good resiliency practices at one point in time from those who can be counted on to have good, ongoing resiliency practices
How does process differ from practice?

<table>
<thead>
<tr>
<th>Process</th>
<th>Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Describes the “what”</td>
<td>• Prescribes the “how”</td>
</tr>
<tr>
<td>• Based on process goals</td>
<td>• No practice goals</td>
</tr>
<tr>
<td>• Manage process to requirements</td>
<td>• Tends toward “set and forget” mentality</td>
</tr>
<tr>
<td>• Select practices based on process goals</td>
<td>• Reinforces domain-driven approach</td>
</tr>
<tr>
<td>• Can be defined, communicated, measured, and controlled</td>
<td>• One size does not fit all</td>
</tr>
<tr>
<td>• Long-lived</td>
<td>• Regulatory vehicle</td>
</tr>
<tr>
<td></td>
<td>• Short-lived</td>
</tr>
</tbody>
</table>
Relationship between process and practice
Embracing process improvement

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

Process maturity increases capability for meeting goals and sustaining the process

“Are we resilient?” or “Are we secure?” is answered in the context of goal achievement rather than what hasn’t happened

Facilitates meaningful, purposeful selection and implementation of practices
Process maturity shifts the paradigm

- No Process
- Partial Process
- Formal Process
- Planned
- Actively managed and controlled
- Cultural

Tactical

Systematic and Adaptive

Irregular and Reactive

Strategic
Process improvement model

Model or framework provides

- A common basis of comparison for planning and benchmarking process improvement

- Defined catalogue of capabilities to guide mastery in a particular domain

- Guidelines and goals for managing, sustaining, and maturing the processes that instantiate the organization’s capabilities
CERT Resiliency Engineering Framework: A process improvement model for resiliency engineering
The Resiliency Engineering Framework

A process framework for resiliency engineering

Defines basic capability areas and provides guidelines for security and business continuity process improvement

Captures vital linkages between security, business continuity, and IT operations

Addresses operational risk management through process management

Establishes a capability benchmark
24 capability areas

Focused on resiliency of people, information, technology, and facilities in the context of services and business objectives
Using the framework

Benchmark current level of capability

Set forward-looking capability 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
Framework status

Currently in outline

Based on resiliency engineering body of knowledge

Version 1.0 to be published this year
Future Plans and Summary:
ongoing work to mature and disseminate the framework
2007 Plans

Continued collaboration with financial sector through FSTC

Complete and publish framework version 1.0

Explore process maturity concepts

Pilot first assessment mechanism

Pilot early training curriculum

Conduct improvement pilots to validate model and approach

Expand REF community
Financial Services Technology Consortium

Member-owned consortium of financial services-focused organizations

Explores new technologies to address industry business needs

**FSTC project participants:**

<table>
<thead>
<tr>
<th>AMD</th>
<th>Discover</th>
<th>KPMG</th>
<th>US Bank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ameriprise</td>
<td>DRII</td>
<td>MasterCard</td>
<td>Wachovia</td>
</tr>
<tr>
<td>Bank of America</td>
<td>DRJ*</td>
<td>Marshall and Ilsley</td>
<td>Wells Fargo</td>
</tr>
<tr>
<td>Bank of Oklahoma</td>
<td>IBM</td>
<td>NY FRB*</td>
<td></td>
</tr>
<tr>
<td>Capital Group</td>
<td>JPMorgan Chase</td>
<td>SunGard</td>
<td></td>
</tr>
<tr>
<td>Citigroup</td>
<td>Key Bank</td>
<td>Trizec Properties</td>
<td></td>
</tr>
</tbody>
</table>

*observing participant
Beyond 2007

Continue outreach and community building

Expand and refine REF product suite

- Model
- Publications
- Training
- Assessment/Appraisal
- Professional certifications for instructors and appraisers

Continued piloting and case study development

Support community adoption
Summary

Today’s environment calls for better operational risk management

Engineering and improving protection and sustainability processes will enhance operational resiliency

REF enables process improvement and benchmarking of operational resiliency capabilities
How can you be involved?

Add your name to our mailing list to be informed when the framework and other project artifacts are available

Participate in a pilot assessment

Explore other forms of collaboration
For more information

David W. White
Software Engineering Institute
Carnegie Mellon University

www.sei.cmu.edu
www.cert.org
dwhite@cert.org