

# ROI – Return on Investment Lessons from Defending Cyberspace

Andy Purdy, Esq., CISSP  
President, DRA Enterprises, Inc.  
BigFix Executive Advisory Board  
[www.andypurdy.com](http://www.andypurdy.com)  
Allenbaugh Samini, LLP  
[www.alsalaw.com](http://www.alsalaw.com)



Committee

# Summary – ROI Perspective

- What approach should we take?
- What risk capabilities do we need?
- Risk management – for organizations and countries
- How should we approach CIIP from a risk and preparedness perspective?

# What risk capabilities do we need?

- Participation by key stakeholders in the organization for risk and response and recovery
- Commitment to assess, prioritize, and implement measures to mitigate risk
- Situational awareness
- Analytical and forensic capabilities
- Incident response capability

# Applying Lessons to Promote ROI

- Build security into the business
  - Engage representatives of key business and other internal units
  - Pursue a process improvement approach to enhance coordination/integration of:
    - security,
    - disaster recovery,
    - business continuity, and
    - IT operations

# Promoting ROI

- Efficiently Manage Risk
  - Identify and implement requirements for situational awareness; pursue technologies that tell you in real time:
    - What is connected to the network;
    - What are the security characteristics of those entities; and
    - Is the device in compliance.
  - Pursue technologies that not only bar noncompliant devices from the network, but – more importantly – put the devices in compliance.

# Example

- CERT® Resiliency Engineering Framework (REF)© created by Carnegie Mellon University and the Financial Services Technology Consortium

©*Copyright 2007 Carnegie Mellon University*

# 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

# Defining the problem©

- Typical organizational approach to operational risk management activities:
  - Poorly planned and executed function
  - Business units not involved
  - No asset management function
  - Seen as a technical function or responsibility
  - Searching for magic bullet: CobiT, ITIL, ISO17799, NFP1600
  - Poorly defined and measured goals
  - Funding model reactive, not strategic

# Why use a “model” 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

# Defining a process approach<sup>©</sup>

- Elevating the management and coordination of operational-resiliency focused activities to the enterprise level
  - Shared goals and resources
  - Elimination of redundancy and stovepipes
  - Elimination of framework quagmire through practice integration
  - Measuring process effectiveness
  - Moving toward process improvement

# Limitations of best practices©

- Best practices are
  - effective ways to approach improvement in a critical organizational activity, like security
- Best practices *ARE NOT*
  - a substitute for an actively planned and managed process

# What is resiliency engineering?©

- The process by which an organization establishes, develops, implements, and manages the operational resiliency of services, related business processes, and associated assets
- “Requirements-driven security and business continuity”

# The Resiliency Engineering Framework<sup>©</sup>

- A framework of practice for integration of security and business continuity activities toward achievement of operational resiliency
- Defines basic process areas and provides guidelines for security and BC/DR process improvement
- Captures vital linkages between security, BC/DR, and I/T ops in the process definition
- Addresses operational risk management through process management
- Establishes a capability benchmark

# 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

# Using the framework<sup>©</sup>

- 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

# REF Summary<sup>©</sup>

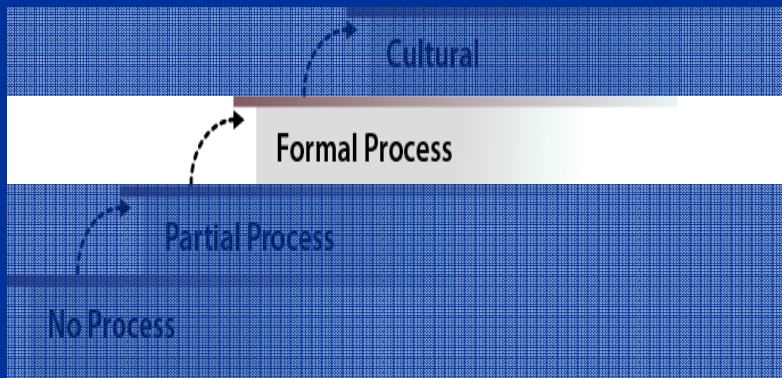
- Operational resiliency must be actively managed
- Security, BC/DR, and IT Ops must collaborate
- Model-based process improvement brings defined, systematic, repeatable, consistent, and improvable processes
- Approach must be flexible and adaptable
- No one-size-fits-all solution

# Formal process<sup>©</sup>

- *Performed and managed*
- *Repeatable*
- *Spans enterprise*
- *Not completely ingrained in culture*
- **RISK-DRIVEN**

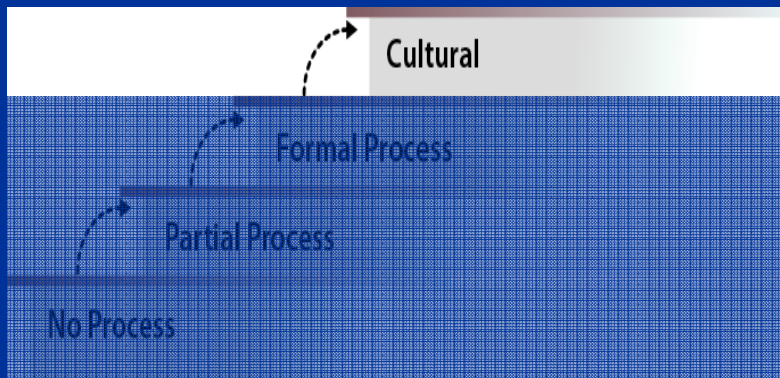
- **Common attributes:**

- Focus on critical assets
- Responsibility of key organizational managers and IT
- Funded as an expense
- Implicit alignment to strategic drivers
- Dependent on localized risk management
- Informal governance, possibly CRM



# Cultural©

- *Performed and managed*
- *Repeatable and proactive*
- *Spans and involves enterprise*
- *Continually measured and improving*
- *Fundamental to organizational success*
- *ENTERPRISE-DRIVEN*



- Common attributes:
  - Focus on critical assets, processes, strategic drivers
  - Responsibility of high-level executive
  - Capitalized
  - Explicit alignment to strategic drivers
  - Reliant upon enterprise capabilities
  - Formal governance and feedback

# Future plans

- Release draft framework to community (early 2008)
- Continue development of process improvement and maturity concepts (throughout 2008)
- Develop appraisal methodology for standardized benchmarking (currently underway)
- Deliver fundamentals training (mid 2008)
- Expand user community through expanded benchmarking efforts (throughout 2008)
- Begin licensing and transition activities (late 2008, early 2009)

# Financial Services Technology Consortium

- Member-owned consortium of financial services-focused organizations
- Explores new technologies to address industry business needs

AMD

DRII

KPMG

US Bank

Ameriprise

EMC

MasterCard

Wachovia

Bank of  
America

IBM

Marshall and  
Isley Bank

Capital Group

JPMorgan  
Chase

NY FRB\*

Citigroup

Key Bank

PNC Bank



Discover

© 2008 FSTC. All rights reserved.

# Participation benefits

- Opportunity to shape and develop model
- Access to early artifacts and discoveries before exposure to larger community
- Early benchmarking and improvement opportunities for their organizations
- Ability to educate and catalyze their organizations on movement toward convergent view
- Take advantage of collaboration with peer organizations solving similar problems

# For more information



- Rich Caralli
- Software Engineering Institute  
Carnegie Mellon University

Kelly Kimberland, APR  
SEI Public Relations  
Manager

Tel: 412-268-8467

[public-relations@sei.cmu.edu](mailto:public-relations@sei.cmu.edu)

- [www.sei.cmu.edu](http://www.sei.cmu.edu)
- [www.cert.org](http://www.cert.org)
- [rcaralli@cert.org](mailto:rcaralli@cert.org)

- Charles M. Wallen
- Financial Services  
Technology Consortium

- [www.fstc.org](http://www.fstc.org)
- [charles.wallen@fstc.org](mailto:charles.wallen@fstc.org)



## Contact information:

Andy Purdy - President, DRA Enterprises, Inc.

BigFix, Inc. Executive Advisory Board

Allenbaugh Samini, LLP ([www.alsalaw.com](http://www.alsalaw.com))

For technology solutions and for information about  
DRA Associates, Inc., visit:

[www.andypurdy.com](http://www.andypurdy.com)

[Andy.Purdy@andypurdy.com](mailto:Andy.Purdy@andypurdy.com)