Auditing Enterprise Resilience

By Richard Cascarino
and Stephen Gierach

Company Backgrounds

Executive Compumetrics, Inc.	Richard Cascarino & Associates
Executive Compumetrics, Inc. (ECI), based in Illinois, has been serving the industry for more than 20 years. During that time, ECI has provided consulting services to a wide variety of IT users, including financial institutions, a major securities exchange organization, life and health insurance companies, property/ casualty insurance companies, power utilities, a "big six" public accounting firm, light and heavy manufacturing companies, food processing and distribution companies, and major telephone utilities.	Richard Cascarino & Associates has, for the last 20 years, been providing Internal Audit, Fraud Audit, IS Audit Consultancy, Risk Management and Corporate Governance consultancy as well as Professional Development services to clients throughout the United States of America, the African region, Europe and the Middle East. These include some of the largest corporations, government departments, auditors general, professional bodies and financial institutions in their respective countries.

Company Backgrounds (cont.)

Executive Compumetrics, Inc.	Richard Cascarino & Associates
The Firm has specialized in — • Organizational Resilience Reviews • Risk Assessment • Physical/Logical Security Assessments • Business Continuity & Disaster Recovery Planning Audits, Testing, & Automation • Third Party Internal Audit and Compliance Management Services • Sarbanes-Oxley Compliance Audit Readiness Services • Model Audit Rule Compliance Audit Readiness Services • SAS-70 Services • Application Control and ERP Reviews • IT and business process re-engineering • Cost reduction analysis	Richard Cascarino & Associates strives to serve its customers by providing high grade, international consulting services in the fields of: • Enterprise Resilience • Enterprise Risk Management • Risk Management • Corporate Governance • Internal Audit • Internal Audit Training • IS Audit • IS Audit Training • Forensic Audit and Fraud Audit • Forensic Audit Training • Fraud Audit Training • Strategic use of IT • Audit Committee effectiveness

The Webinar will Cover:

- The seven strategic risk classes
- Disintegration of Business Processes
- Establishing areas of corporate vulnerability
- Driving business value through the supply chain
- Integrating people, processes, and data
- Re-engineering the Internal Audit Approach

What is Resilience?

- Resilience is the ability of an organization to provide and sustain an acceptable level of service in the face of various major faults and challenges to normal business operation

What's at Risk?

- Trust
- Reputation; brand
- Shareholder/stakeholder value
- Market confidence, share, capitalization
- Regulatory compliance; fines, jail time
- Customer retention, growth
- Customer and partner identity, privacy
- Ability to offer, fulfill business transactions
- Staff morale

Varying Views of Risk

- **Engineering**: (Probability of an accident) x (loss per accident)
- **Military**: (Capability of enemy) x (Enemy intent)
- **Finance**: Unexpected variability or volatility of returns (positive or negative)
- **Statistics**: Probability of some event which is seen as undesirable
- But what about:
  - Technological Discontinuities
  - No active risk management plan
  - Regulatory Upheavals and Significant Compliance Deficiencies
  - Geopolitical Shocks, labor strikes, and unanticipated economic downturns
  - Abrupt shifts in consumer tastes
  - Non-traditional competitors, cartels, regional monopolies
  - Disruption of essential services
  - Unauthorized disclosure of Intellectual Property
  - Corporate lawsuits in federal civil court, demanding forensic discovery

Normal Classifications of Strategic Risk

- Industry
- Technology
- Brand
- Competitor
- Customer
- Investments: Projects; Acquisitions; R&D
- Stagnation

Why not just "Survival of the Fittest"?

- OK unless you are a dinosaur
- Natural selection not always an effective approach to developing organizational capability
  - Cost of organizational failure is high
    - in human terms
    - in lost confidence
  - But how do we ensure renewal and adaptation?

Traits of Enterprise Resilience

- Use a wide array of information
- Generate a portfolio of strategic options
- Remain aware of industry breakpoints
- Develop effective governance & risk processes
- Separate corporate and business strategy
- Align with multiple environments
- Develop a strong business purpose & values
- Manage the business as a portfolio – one size does NOT fit all

Barriers to Enterprise Resilience

- Seen as abstract and concerned with low probability hypothetical events
- Requires an holistic, enterprise-wide problem; not just technical
- No widely accepted measures/indicators/metrics
- Focus on disaster-preventing rather than payoff-producing (like insurance)
- Installing security safeguards can have negative aspects (added cost, diminished performance, inconvenience) and be ineffective against actual risks
- Inadequate or lack of reserve funds set aside to deal with one or more significantly impacting concurrent/cascading events

What is a Resilient Enterprise?

- **A Resilient Enterprise Is Able To. . .**
  - withstand systemic discontinuities and adapt to new risk environments [Starr]
  - be sensing, agile, networked, prepared [Starr]
  - dynamically reinvent business models and strategies as circumstances change [Hamel]
  - Have the capacity to change before the case for change becomes desperately obvious [Hamel]

Starr, Randy; Newfrock, Jim; Delurey, Michael. "Enterprise Resilience: Managing Risk in the Networked Economy." strategy+business, Spring 2003. Also appears in "Enterprise Resilience: Risk and Security in the Networked World: A strategy+business Reader." Randall Rothenberg, ed.

Hamel, Gary; Valikangas, Lisa. "The Quest for Resilience," Harvard Business Review, September 2003

Developing a Resilience Strategy

- Overall Aim: To improve the enterprise resilience by building the capabilities needed to absorb, respond to and recover from disruptive challenges
  - Effective short term horizon scanning and medium term risk assessment at international, national, regional and local levels
  - Readiness to respond to disruptive challenges and provision of an effective and coordinated crisis management response

Developing a Resilience Strategy

- Assessment of any required generic capability of emergency services and other category 1 responders to deal with the full range of localized emergencies
- Specific plans for those risks, judged by the enterprise, to have significant or catastrophic impacts upon it
- Enhanced business continuity management to maintain provision of services or recovery as quickly as possible
- Community resilience encompassing local organizations as well as communities, families and individuals.

An Effective Approach

- Sets the board risk agenda, and heightens awareness and transparency around material risks and efforts to manage them
- Enhances business discipline and internal controls
- Ensures informed decision-making to strengthen strategic response plans and overcome potential obstacles to meeting corporate performance objectives
- Aligns risk management activity with board and management risk agendas and reconciles risk management priorities with strategic imperatives
- Improves effectiveness of risk control investments
- Provides ample reserve funds set aside to support the response/ recovery plan execution

An Effective Approach

- Establishes a culture that embodies a common vision and taxonomy for managing and thinking about risk
- Protects directors and officers against charges of lack of good faith or due diligence and preserves for directors and officers the benefit of the "business judgment" rule
- Improves corporate performance and supports shareholder value and builds stakeholder trust (e.g., investors, strategic partners)

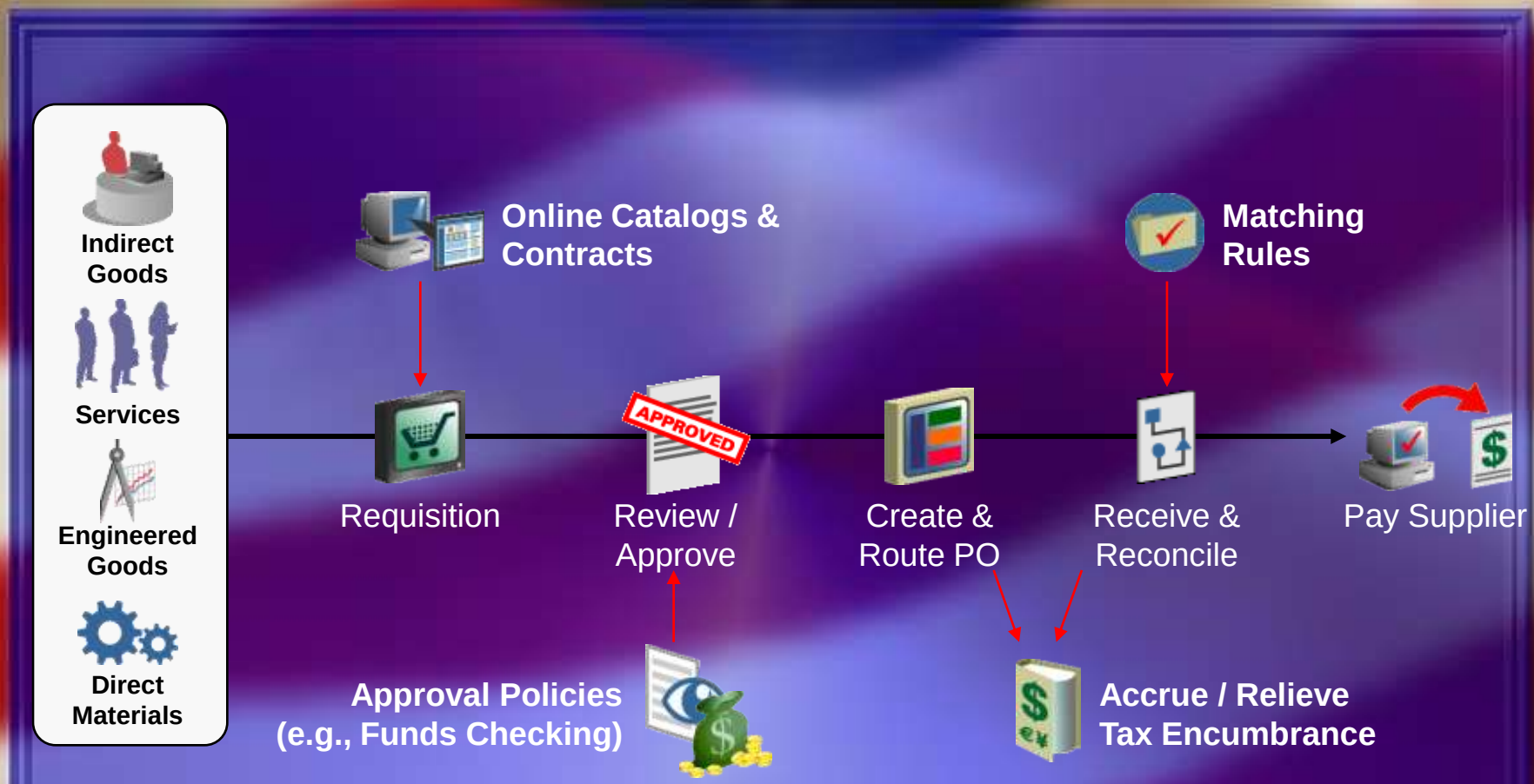
An Effective Resilience Strategy Involves

- Vision, Mission & Strategy
- Culture & Communication & Toolboxes
- Structure
  - Corporate Governance
  - Management Team
  - Processes
- Flexibility
  - Know your cyclicality
  - Build flexibility in good times to respond to bad times: create buffer

Monitoring and Response

- Continuously monitor environment looking for event pre-cursors and threshold exceptions
  - Cross-functional decision making
  - Max Weber's assertion that those with the most relevant expertise should take the decision making lead has been outdated by modern information systems and the understanding of decision making
  - Multiple information sources gives richer information
  - Avoids the risk of being advised by those that have a vested interest in the status quo
  - Avoids "*Locally Rational*" decision
  - Portfolio of Strategic Options
  - Tighter corporate governance
    - To "*focus the mind*"

Supply Chain Resilience



Beware of:

- Do suppliers have effective BCP themselves
- No Single Point of Failure
  - Have multiple suppliers identified
  - Have signed contracts in place

Internal Audit's Role

- Leverage Audit's professionalism and enterprise-wide scope
  - Supplement compliance activities with risk assessment and process improvement
  - Create an enterprise-wide risk-based audit program
  - Broaden audit scope to address third-party and vendor risk
  - Collaborate with Risk Management
  - Obtain & assess adequacy of SAS-70 reports of outsourcing firms
  - Ensure that the organization's inventory of available internal resources and vendor suppliers are actively maintained
  - Require vendor suppliers to maintain a tested BCP
  - Re-examine the adequacy of existing insurance coverage

Reinventing Internal Audit

- **"We trained hard, but it seemed that every time we were beginning to form up into teams, we would be reorganized. I was to learn later in life that we tend to meet any new situation by reorganizing, and a wonderful method it can be for creating the illusion of progress while producing confusion, inefficiency and demoralization"**

Petronius Arbiter, 66 AD

How the Auditor can Hinder

- Insist on the old ways
- Focus on procedures rather than objectives
- Make Effectiveness the bottom priority
- Insist on straightjacket controls
- Get in the way
- Stay out of the way

Where do we start?

First, develop an overarching *enterprise risk model* that is –

- **Comprehensive and consistent with the mission and values of the organization, and**
- **Widely accepted within the organization**

Where do we start?

- **Look for clear and direct lines of authority with dedicated staff for Resilience, and ensure that responsibility and authority for security is integrated, not dispersed**
- **A strong, accountable advocate at the executive level, with broad corporate acceptance of the role of Resilience at the BOD level in protecting enterprise interests, is vital!**

Where do we start?

- **Seek evidence of Resilience in critical suppliers and partners**
- **Make Resilience Reviews an element of contracts for critical services and periodically evaluate compliance**

Where do we start?

- **Ensure a consistent designation and valuation of critical assets exists**
- **Assess the adequacy of the security program in place to protect the high value assets from known risks/threats**
- **Develop the means to audit the risk resilience of these assets**

Where do we start?

- **Ensure careful consideration is given to resiliency issues associated with any organizational changes is communicated to all staff potentially affected by the changes.**
- **Ensure Resilience becomes part of the corporate culture and corporate goals**

Where do we start?

- **Develop indicators for Resiliency efficiency and performance to ensure a robust program and to ensure that corporate competitive strategies do not undermine overall Enterprise Resilience**

Where do we start?

- **This is not a comprehensive Audit Plan, but rather a starting point**
- **For other information – see**
  - http://www.cert.org/resilience/

Example of Audit Plan

- Determine examination scope and objectives for reviewing the BC planning program.
- Determine the existence of an appropriate enterprise-wide BC plan.
- Determine the quality of BC plan oversight and support provided by the board of directors and senior management.
- Determine whether an adequate BIA and risk assessment have been completed.
- Determine whether appropriate risk management over the BC process is in place.

See IIA G-Tag 10

Example of Audit Plan

- Determine whether the BC plan(s) include(s) appropriate testing to ensure the business process(es) will be maintained, resumed, and/or recovered as intended.
- Determine whether the IT environment has a properly documented BC plan that complements the enterprise-wide and other departmental BC plans.
- Determine whether the BC plan(s) include(s) appropriate hardware backup and recovery.
- Determine whether the BC process includes appropriate data and application software backup and recovery.

See IIA G-Tag 10

Example of Audit Plan

- Determine whether the BC plan(s) include(s) appropriate preparation to ensure the data center recovery processes will work as intended.
- Determine whether the BC plan(s) include(s) appropriate security procedures.
- Determine whether the BC plan(s) address(es) critical outsourced activities.
- Discuss corrective action and communicate findings.

See IIA G-Tag 10

Resilience involves re-engineering Paradigms

- **Current paradigms**
  - **Internal control = Management control**
  - **Management control starts with governance**
  - **Top management can control everything**
  - **Internal control is imposed**
- **Re-engineered Paradigm**
  - **Resilience focuses control with owners of the process**
- **Role of Internal Audit must change to reflect the new reality**

Where We can Help

- Conduct a situation assessment of progress and gaps identified & weighted. Identify areas of project high risk.
- Review/assess and modify/enhance/refocus the current Internal Audit program/process and project plan, directing committee, team organization, and resource requirements to Enterprise Resilience
- Develop a response/action plan, as needed, to prioritize, and coordinate each functional phase with suitable resources, milestones, and deliverables
- Perform simulated situation testing to assure the effectiveness of the organization's resiliency plans, including participation with public authorities

Where We can Help

- Provide remediation Quality Assurance & Oversight support to ensure all control gaps are adequately fixed
- Provide independent testing of modifications/changes made in terms of –
  - Effectiveness of Design
  - Effectiveness of Operation
- Provide Project Management and technical assistance for Enterprise Resilience Auditing, process design, development, & implementation.

Thank you for Listening

We can help your organization to maintain its competitive advantage by ensuring that Internal Audit appropriately addresses the Enterprise Resilience approach

Please feel free to contact us at:

Richard Cascarino & Associates

PO Box 775524
Steamboat Springs
(970)291 1497
www.rcascarino.com
info@rcascarino.com

Executive Compumetrics, Inc.

P. O. Box 95
Tinley Park, IL 60477
(708) 633-1190
www.ExeCompInc.com
steve@ExeCompInc.com