

# Prepare.

**Briefing Materials**

Workshop on Risk Intelligence and Resilience



**Compete.**

Council on  
Competitiveness

## **Briefing Materials**

### Workshop on Risk Intelligence and Resilience

**EDITED BY Debbie van Opstal**, Senior Vice President,  
Policy and Programs, Council on Competitiveness

This publication may not be reproduced, in whole or in part, in any form beyond copying permitted by sections 107 and 108 of the U.S. copyright law and excerpts by reviewers for the public press, without written permission from the publishers.

The Council on Competitiveness is a nonprofit, 501 (c) (3) organization as recognized by the U.S. Internal Revenue Service. The Council's activities are funded by contributions from its members, foundations, and project contributions. To learn more about the Council on Competitiveness, visit us at [www.compete.org](http://www.compete.org).

**COPYRIGHT** © 2008 Council on Competitiveness

**DESIGN** Soulellis Studio

# Prepare.

**Briefing Materials**

Workshop on Risk Intelligence and Resilience





**Prepare.**

## Table of Contents

Letter from the President	4
Understanding Risk Intelligence and Resilience	5
Summaries of Seminal Articles/Surveys/Books	
Warning: Turbulence Ahead	7
Capturing Value from Risk Intelligence and Resilience	11
Implementing Risk Intelligence	16
Reaching for Resilience	26
Roles for Governance	38
Recommendations for Risk Intelligence and Resilience	46
About the Council on Competitiveness	62

## Letter from the President

I am pleased to present Prepare, a collection of current thinking and best practices on a key competitiveness driver: risk intelligence and resilience. Prepare was initially developed as a briefing book for participants in the Risk Intelligence and Resilience Workshop, held in Wilmington, Del., in October 2008. It reflects seminal research and recommendations on risk management and resilience, governance roles and responsibilities, and opportunities to capture opportunity out of adversity.

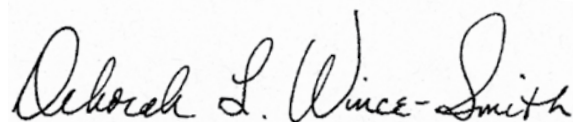
These first years of the 21st century are best described by the three T's: transition, turbulence and transformation. Rapid globalization is altering our world in fundamental ways, and we are more connected and more interdependent than ever before. With these tectonic shifts have emerged new risks that cascade across networks and borders: geopolitical instability and terrorism, energy and resource volatility, pandemic diseases, and new methods of crime, among others. What happens anywhere can have profound effects everywhere; when subprime mortgages in the United States failed in 2008, world markets lost more than 16 trillion in just the first 10 months of the year.

While we may not be able to predict the future with great accuracy, one thing is certain: risk management as usual will not be enough to secure competitiveness or security—for either companies or countries. The financial sector was considered the best in class in enterprise risk management. Operational risks—typically a back office function—are becoming “bet the company” risks.

We need a new approach—new insights, new language, new systems and new metrics. The next new revolution in business will be in risk management and resilience. Just as we built integrated quality and safety management systems, so we must now build integrated risk management systems. As we come to manage risk better, we will become more resilient, with systems and processes that are robust, adaptive and flexible, ready to respond on a dime, and resourceful—able to turn adversity into opportunity.

Prepare is a crucial first step in stimulating new thinking. Under the leadership of Chad Holliday, chairman and CEO of DuPont, our Wilmington workshop brought together a wide spectrum of risk managers and risk management experts. We would like to thank Jim Quigley, CEO of Deloitte, and John Swainson, CEO of CA, for their sponsorship of this opportunity to understand how different risk functions link to each other and to strategic planning and what CEOs and boards need to know about risk management. Debra van Opstal ably led the Council team, with the help of David Padgham, Mildred Porter and Michael Ruthenberg-Marshall.

Sincerely,



Deborah L. Wince-Smith

## Section 1

# Understanding Risk Intelligence and Resilience

## The Challenges

### Turbulence

Hamel and Valikangas, *Quest for Resilience*

The world is becoming turbulent faster than organizations are becoming resilient. Technological discontinuities, regulatory upheavals, geopolitical shocks, industry de-verticalization and disintermediation, abrupt shifts in consumer taste and hordes of non-traditional competitors—these are just a few of the forces undermining the advantages of incumbency.

### Long-Term Sustainability

World Economic Forum

During the last year, a series of risk issues has focused global attention on the fragility of the global system. Uncertainty about the short- and medium-term future is as high as it has been in a decade. Proactive management of globalization to ensure its long-term sustainability may be derailed by the prevailing currents of uncertainty. But, inaction on long-term risks will only weaken the global capacity to manage future challenges. And, under conditions of global stress, one core question becomes more salient: Who owns the risk?

### Predictable Surprise

Bazerman and Watkins, *Predictable Surprise*

Many companies are vulnerable to “predictable surprise”—the disasters leaders could have seen coming but did not. Predictable surprises happen when leaders have all the data and insight they need to recognize the potential for, even the inevitability of, major problems but fail to respond with preventative action.

### Globalization and New Operational Risks

Council on Competitiveness, *Transform*

From a risk management perspective, globalization cuts two ways. On one hand, companies are able to leverage geography to disperse risk. On the other hand, globalization also increases a company’s exposure to disruptions in its operational lifelines—information and communications, supply chain, energy infrastructure disruptions; in transportation, communications, information—that enable the enterprise to operate seamlessly across different geographies. These kinds of operational risks are the fastest growing category of risk. Once considered a problem for the back office, the potential for cascading failure can make them “bet the company” risks.

### Strategic Resilience

Reinmoellere and van Baardwijk, *Resiliency: Business’ Foremost Strategic Goal*

In a turbulent environment, companies need to become more resilient. Strategic resilience is not about responding to a one-time crisis. It is not about rebounding from a setback. It is about continuously anticipating and adjusting to deep, secular trends that can permanently impair the earning power of a core business. It is about having the capacity to change before the case for change becomes desperately obvious.

## Workshop Concept

On October 30 and 31, 2008, more than 60 corporate leaders and academics gathered in Wilmington, Del., to explore ideas and share best practices on risk intelligence and resilience. Their discussions centered on three key themes:

### 1. Define a Common Lingo

The business world is in a Tower of Babel. People who use the risk, security and resilience terms can mean vastly different things while people who use different words actually have the same objectives. Words matter, and everyone needs to be on the same page.

**Goal:** To reach a common definition by describing the desired end state

**Define:** A language of risk: governance, risk management, resilience, compliance.

### 2. Develop a Dashboard

Metrics help determine whether an organization has actually achieved the desired state—measures that can be used by boards or CEOs to determine the level of resilience of the enterprise or to calculate the bottom-line benefits/shareholder value.

**Goal:** Describe a dashboard that would enable CEOs and boards to know that they are managing risk effectively and that the enterprise is resilient. Outcomes may not always be directly realized in the top- or bottom-line, so a variety of benchmarks might be needed to justify investments in resilience.

**Develop:** Specific measures/metrics that create a standardized system for risk awareness and monitoring, and propose practices that executives could use to justify “cost of resilience” with their shareholders.

### 3. Deploy Policies that Reinforce Market Mechanisms

What role should the markets play in helping to move organizations toward more risk intelligence and resilience? What can the government do to reinforce private sector drivers and market mechanisms that encourage/reward investments in resilience and risk intelligence?

**Goal:** Describe private sector actions/public policies that would reinforce rewards for risk intelligence and resilience. Examine how homeland security policies and investments can reinforce economic security.

**Deploy:** Policies that encourage market-movers and shareholders to reward resilience.

### CEO and Board Perspectives on Risk

During the workshop, CEOs and board members, including Charles O. Holliday, Jr., CEO of DuPont, Tom O'Neill, principal of Sandler O'Neill, Mark Layton, vice chairman, audit of Deloitte & Touche, LLP, Larry Rittenberg, chairman of COSO, and Deborah L. Wince-Smith, president of the Council on Competitiveness, came together to discuss the questions boards are asking (or not asking) about risk exposure and the information they need but are not getting.

## Section 2

# Warning: Turbulence Ahead

### Overview

Globalization, competition, technological complexity, interdependence and speed are fundamentally changing the kinds of risks and competitive challenges that companies—and countries—face. The competition is getting much better. The world is entering an age in which “we’ll all be competing with everyone, from everywhere, for everything”.<sup>1</sup>

Technological complexity and interdependence in the global economy are increasing other risks. Extended and interdependent energy, transportation, information and communications networks can quickly magnify the impact of point failures—whether triggered by attack or accident. Operational risks, once thought to be a back office concern and trivial in comparison to market and credit risks, are becoming bet-the-company risks that belong in the boardroom.

Studies may disagree as to which are the greatest risks, but every study underscores the concern of business executives that risks are rising.

**“It’s a whole new ballgame on risk—for countries as well as companies.”**

*Transform*, Council on Competitiveness

### **Global Risks 2008: A Global Risk Network Report**

World Economic Forum, January 2008

The World Economic Forum (WEF) highlights major categories of transnational risk—with emphasis on systemic financial risk, food security, supply chains and energy. Globalization has increased the likelihood of a “tragedy of the commons”-type outcome by reducing the incentives for any one actor to address problems like pandemics, pollution or global warming. Interdependency has also increased the probability that a disruption in any one region may have significant global repercussions.

The WEF compared the likelihood of 26 core global risks with their predicted severity in terms of economic loss (measured in U.S. dollars).

1. *Globality*, Harold Srikin, James Hemerling and Arindam Bhattacharya. Boston Consulting Group (Boston: 2008)

## Core Global Risks and Predicted Severity

Source: World Economic Forum, January 2008

	Risk	Perceived Likelihood (%-WEF Analysis)	Cost (Severity in Billions of US\$)
<b>Economics</b>	Food Insecurity	5-10	50-250
	Oil and Gas Price Spike	10-20	250-1,000
	Major Fall in US\$	7-12	50-250
	Slowing Chinese Economy (6%)	7-12	250-1,000
	Fiscal Crises in Advanced Economies	1-5	50-250
	Asset Price Collapse	17-22	>1,000
<b>Geopolitics</b>	International Terrorism	5-10	10-50
	Collapse of Nuclear Proliferation Treaty	7-12	5-25
	Interstate and Civil Wars	5-10	50-250
	Failed and Failing States	10-20	30-150
	Transnational Crime and Corruption	5-10	50-250
	Retrenchment from Globalization (Developed)	5-10	>1,000
	Retrenchment from Globalization (Developing)	7-12	50-250
	Middle East Instability	10-20	150-625
<b>Environment</b>	Extreme Climate Change Related Weather	7-12	50-250
	Heat waves and Droughts	7-12	50-250
	Loss of Freshwater	5-10	10-50
	Natural Catastrophe: Cyclone	1-5	50-250
	Natural Catastrophe: Earthquake	1-5	50-250
	Natural Catastrophe: Extreme Inland Flooding	1-5	30-150
<b>Society</b>	Pandemic	5-10	250-1,000
	Infectious Disease, Developing World	3-8	50-250
	Chronic Disease, Developed World	10-20	150-625
	Liability Regimes	5-10	50-250
<b>Technology</b>	CII Breakdown	7-12	150-625
	Emergence of Nanotechnology Risks	1-5	10-150

### **Risk 2018: Planning for an Unpredictable Decade**

Economist Intelligence Unit, 2008

In 2008, the Economist Intelligence Unit (EIU) surveyed 600 senior-level executives to evaluate and rank which risks they believed would present the most significant threats to business during the next decade, as well as the level of preparedness of their individual organizations to address each risk.

#### **High Risk/Impact with Less than High Readiness**

- Climate change
- Retrenchment from globalization
- Oil price shock
- Instability in Middle East
- Asset price collapse
- International terrorism
- Emergence of disruptive business mode

#### **High Risk/Impact with High Readiness**

- Unexpected regulatory change
- Global recession
- Increased competition from emerging market economies
- Talent shortages

The EIU survey noted that: "Risk management appears to be a function in transition. While it retains its responsibilities as a source of assurance that ensures regulatory compliance and helps the orga-

nization to avoid loss, it is now expanding beyond this traditional heartland to assume a broader role. Among our survey respondents, there is general agreement that risk management will encompass more strategic activities over the next ten years, with two-thirds expecting an increase in the use of risk management as a strategic tool."

Risk management and controls now have two parallel dimensions: the traditional "keep me out of trouble" side of risk and the emerging "make my business better" aspect. Managing risk effectively can help improve performance, help improve process and strengthen competitive advantage.

### **Strategic Business Risks 2008**

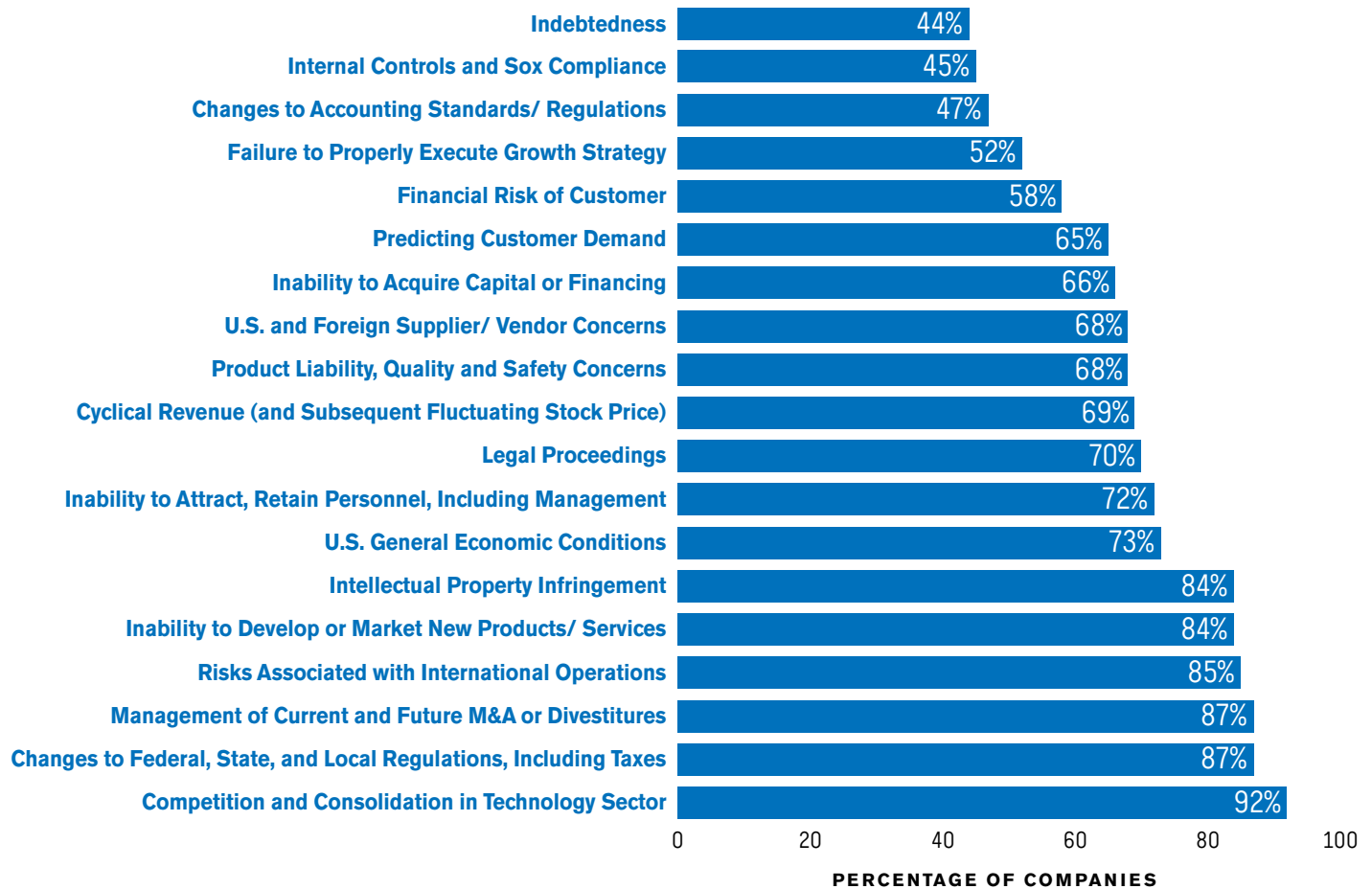
Ernst & Young

Interviews with more than 70 analysts across 20 disciplines by Ernst & Young captured a different set of insights on key risks.

- Regulatory and compliance risk
- Global financial shocks
- Aging consumers and workforce
- Inability to capitalize on emerging markets
- Industry consolidation/transition
- Energy shocks
- Execution of strategic transactions
- Cost inflation
- Radical greening
- Consumer demand shifts

## Top 20 Risks U.S. Tech Companies are Losing Sleep Over

Source: CMP Techweb, May 28, 2008. Based on an analysis of 10K filings.



### Section 3

# Capturing Value from Risk Intelligence and Resilience

## Overview

A key theme is that risk management is not just about minimizing losses, but about preserving shareholder value and growing the top line. The first wave of studies extended the lens beyond simply calculating immediate losses from failure in risk management. They linked risk management to long-term earnings and shareholder value. A next wave of studies is needed for a more rigorous examination of the upside potential for value creation.

## Disarming the Value Killers

Deloitte & Touche, 2005

The Deloitte study found that many of the largest losses in value among the world's largest global companies resulted from their failures to manage risk effectively and systemically. Almost half of the 1,000 largest global companies suffered declines in share prices of more than 20 percent in a one-month period between 1994 and 2003, relative to the Morgan Stanley Capital International (MSCI) World Index. And the value losses were often long-standing. Roughly one-quarter took more than a year for their share prices to recover, sometimes much longer. By the end of 2003, share prices for one-quarter of these companies had not recovered to their original levels.

**“A risk intelligent enterprise knows when to avoid danger and when to take a chance. It doesn't just stay in business. It prospers.”**

*James Quigley, CEO Deloitte  
Fortune Magazine, “Weathering Any Storm”, March 19, 2007*

The study found that most firms were exposed to more than one type of risk—whether strategic, operational, market or financial—and failed to manage the relationships among these different types of risk. Actions taken to address one type of risk had the potential to increase exposure to other types of risk.

## Countering the Biggest Risk of All

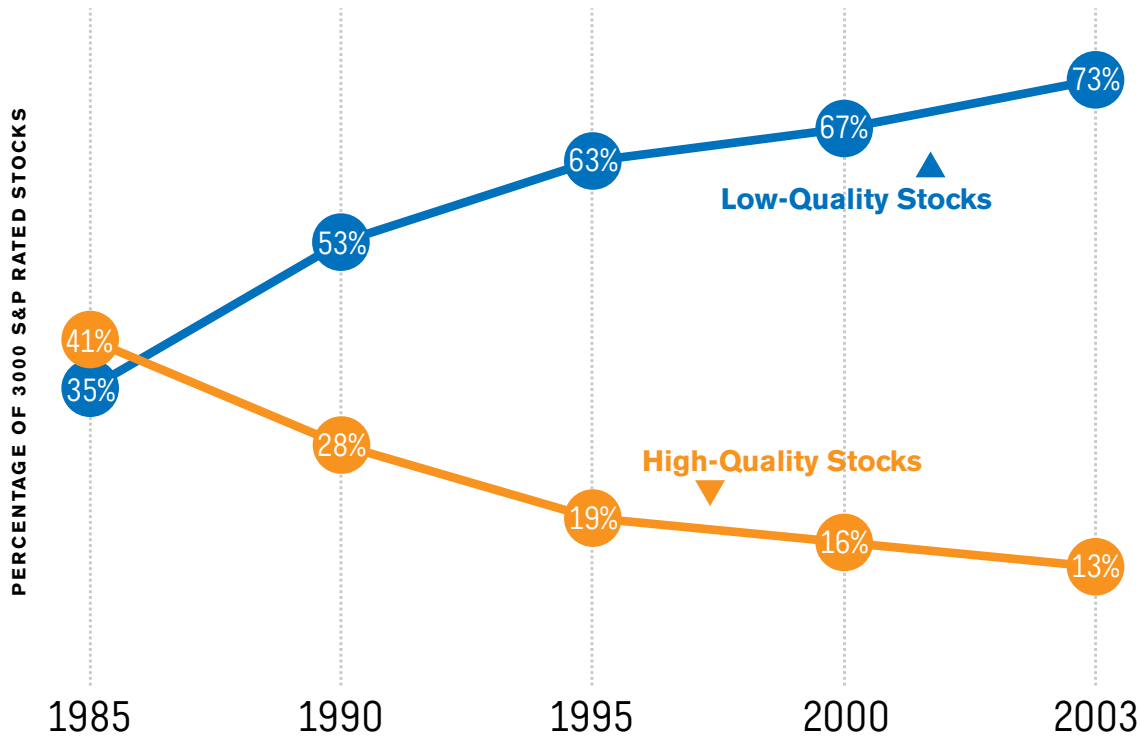
Adrian Slywotzky and John Drzik  
Harvard Business Review, April 2005

The evidence of strategic risk is becoming ever more apparent. In the past 20 years, there has been a dramatic decrease in the number of stocks receiving a high quality rating by Standard & Poor's and a dramatic increase in the number of low-quality stocks. From 1993-2003, more than one-third of Fortune 1000 companies lost at least 60 percent of their value in a single year.

Many firms have been adopting the practice of enterprise risk management—focusing on financial, hazard and operational risks—but most managers have not systemically addressed the strategic risks

## Strategic Risks are Growing

Source: Harvard Business School Review, April 2005



**Note:** High-quality stocks include those rated A+, A and A-. Low quality stocks include those rated B, B-, C and D.

that can be a more serious cause of value destruction. The authors categorize strategic risk into seven major classes: industry, technology, brand, competitor, customer, project and stagnation.

Managing for strategic risks can often turn defensive moves into offensive opportunities. Besides limiting the downside, strategic risk management helps managers improve the odds of success by forcing them to think more systematically about the future and helping to identify opportunities for growth.

Airbus's focus on a collaborative model that would help its member companies to escape shrinking margins enabled it to create sufficient market share to become a true rival to Boeing. For American Express,

the fundamental change in its brand investment mix, in response to competitive threats from other bank cards, set off a decade of growth. For Target, shifting its focus to a customer segment that was different from Wal-Mart's not only helped it sidestep a new competitor but sparked profitable growth.

While managers often see a trade-off between risk and reward, creative risk management combined with a good business model can allow a company to improve in both areas. This is analogous to the evolution, 30 years ago, from a cost-quality trade-off to total quality management which achieved lower costs and higher quality simultaneously.

### **The Effect of Supply Chain Disruptions on Long-Term Shareholder Value, Profitability and Share Price Volatility**

Vinod Singhal and Kevin Hendricks  
The Logistics Institute 2005

Researchers looking at the impact of supply chain disruptions found that such events can be catastrophic for businesses and their shareholders. Based on a sample of more than 800 companies that announced a supply chain disruption between 1989 and 2000, 33-40 percent experienced lower stock returns than their industry peers, regardless of industry, cause of disruption or time period. Such firms experienced 7 percent lower sales growth and 11 percent higher costs.

The study shows that firms that experience disruptions, on average, experience a 107 percent decrease in operating income, 114 percent decrease in return on sales, and 92 percent decrease in return on assets. Changes in operating income, sales, total costs and inventories remained negative in the two years after the problems were disclosed.

### **Innovators in Supply Chain Security: Better Security Drives Business Value**

Stanford and Manufacturing Research Institute, National Association of Manufacturers, 2006

International trade is no longer just about moving goods quickly and cheaply. In this age of global terrorism, there is a third element: it is about moving goods quickly, efficiently and securely. Some of the implications of the 9/11 events include an increase of 15 percent in airfreight costs and an increase of 20 percent in the costs of commercial insurance premiums to about \$30 billion per year. New security measures following 9/11 are estimated to cost the U.S. economy alone more than \$150 billion, of which \$65 billion is for changes in supply chains.

The study also quantified benefits, through case studies of eleven major manufacturers and three logistics providers, that have the potential to offset or exceed the costs of security, including:

- Improved product safety (38 percent reduction in theft/loss/pilferage, 37 percent reduction in tampering);
- Improved inventory management (14 percent reduction in excess inventory, 12 percent increase in reported on-time delivery);
- Improved supply chain visibility (50 percent increase in access to supply chain data, 30 percent increase in timeliness of shipping information);
- Improved product handling (43 percent increase in automated handling of goods);
- Process improvements (30 percent reduction in process deviations);
- More efficient customs clearance process (49 percent reduction in cargo delays, 48 percent reduction in cargo inspections/examinations);
- Speed improvements (29 percent reduction in transit time, 28 percent reduction in delivery time window);
- Resilience (close to 30 percent reduction in problem identification time, response time to problems and in problem resolution time); and
- Higher customer satisfaction (26 percent reduction in customer attrition and 20 percent increase in number of new customers).

# The New Religion of Risk Management

**Peter Bernstein**

Harvard Business Review, March-April 1996

The notion that the future rests on more than just a whim of the Gods is a young idea. More than any other development, the quantification of risk defines the boundary between modern times and the rest of history. What have we gained in the transformation from superstition to the supercomputer? We must consider the possibility that breaking free from the Fates has turned us into slaves of a new kind of religion, a creed that is just as implacable, confining and arbitrary as the old.

All but two of the risk management tools we employ today, from the strict rationality of game theory to the challenges of chaos theory, stem from developments between 1654 and 1754. These methods allow people to take more risks than they otherwise would—a benefit to society which cannot progress without risk takers. Without the laws of probability, no great bridges would span our widest rivers, polio would still be crippling children and no airplanes would fly. Without fire insurance, only the wealthiest could afford to own homes. The great capital-intensive industries of our age, such as the railroads and electric power, would have been inefficient creations of the state or not developed at all.

But, there are inherent risks in our risk management tools: the exposure to discontinuity, the arrogance of quantifying the unquantifiable and the threat of increasing risk instead of managing it.

**Discontinuity** The amazing stability of key relationships depletes the capacity of people to imagine anything different. Many calamities are not unpredictable; they have just become unthinkable.

**Quantifying the Unquantifiable** How can we instruct a computer to model events that have never occurred? Instead, we only program past data, limiting our deliberations to the variables that lend themselves to quantification.

**Increasing the Risk** Our faith in risk management tools encourages us to take risks, but we should be wary of increasing the total amount of risk. Seat belts can cause drivers to behave more aggressively. Derivative instruments to hedge risk have become vehicles for high-speed sleigh rides. Diversification is no guarantee against loss, only against losing everything at once.

Nothing is more soothing and authoritative than the screen of the computer with its imposing arrays of numbers, luminous color schemes and artfully composed charts. We tend to forget that we are operating a gadget whose mind is at rest. Computers exist to answer questions, not to ask them. Whenever we allow ourselves to ignore that truth, the computer becomes the ally, rather than the enemy, of our conceptual errors.

## The Business Value of Resilience

Council on Competitiveness, *Transform*.

Company Vignettes

### Wal-Mart

Wal-Mart's reputation for supply chain gymnastics was showcased during Hurricane Katrina, when the company was able to bring 66 percent of its stores in the affected region back into operation with 48 hours, and 93 percent within seven days. But, its supply chain sophistication was not developed as a disaster management tool—and in fact, the investment could not have been justified solely on disaster preparedness grounds.

The inventory visibility and supply chain agility is rooted in a business model that requires quick changes in the merchandise mix as a source of competitive advantage and new business opportunities, and robustness in its information and logistics systems. Resilience has been embedded in the company's DNA to handle peak requirements.

### Georgetown

The availability of student housing is a critical part of the university's business continuity. If housing is not available, then one of the main sources of operating revenue—tuition—is also at risk. Georgetown undertook a project to improve residence hall safety standards that exceeded code—installing sprinklers and other equipment—resulting in a significant decrease in its insurance premiums. The university took these savings and increased its business interruption insurance fivefold (well before Katrina).

That became a positive factor in determining the university's rating and cost of capital in a subsequent bond issue.

### Waste Management

After 9/11 and a break-in a few months later at a landfill in Cut and Shoot, Texas, that destroyed half a million dollars in heavy equipment, Waste Management began to investigate the benefits of a state-of-the-art security operations center. It found that its own security was inconsistent across its 2,000 facilities. Some facilities lacked alarms altogether, and other alarms were broken or not in use. So, the company created the Life Safety Control Center (LSCC) and deployed smart video and alarm technologies to monitor intrusions into secured areas, as well as to monitor for fire or workplace violence. The LSCC is creating benefits for the company that go well beyond security, including reduced fraud and new tools for work process efficiency and safety. New business opportunities have included a "witnessed and certified" product destruction service, and security contracting for small and medium size companies. The security center has gone from an overhead expense to a profit center for the company.

## Section 4

# Implementing Risk Intelligence

**“Risk comes from not knowing what you’re doing.”**

*Warren Buffett*

**“A little risk management saves a lot of fan cleaning.”**

*Unknown*

## Overview

How firms should manage risk remains a hotly debated topic. Enterprise Risk Management (ERM) was assumed to be the best practice...at least until the subprime crisis. What seems clear is that, even despite the debacle, the tools, talent and processes for market and credit risk management are still more sophisticated than those available for operational risk or strategic risk management.

The literature on ERM seems to fall into three separate categories:

1. ERM is a good approach, but it has never been fully implemented and risks remain siloed;
2. ERM is fundamentally flawed; the approach ignores risk intelligence in favor of risk assessment. Business managers on the ground are in a far better position to sense and understand risk than a headquarters-based risk management system; and
3. ERM approaches, even if well implemented, are incomplete. Perfect risk management will still be ineffective if the processes are not linked to governance, strategic planning and value creation.

### ERM Just Needs to Be Fully Implemented

#### Does ERM Matter? Enterprise Risk Management in the Insurance Industry

PriceWaterhouse Coopers, June 2008

Key findings from a survey of 53 insurers:

The extent to which ERM is integrated into the day-to-day decision-making and frontline risk-taking of businesses is often limited. Less than half of the survey participants are confident that ERM has been embedded into their strategic planning, resource allocation and performance management.

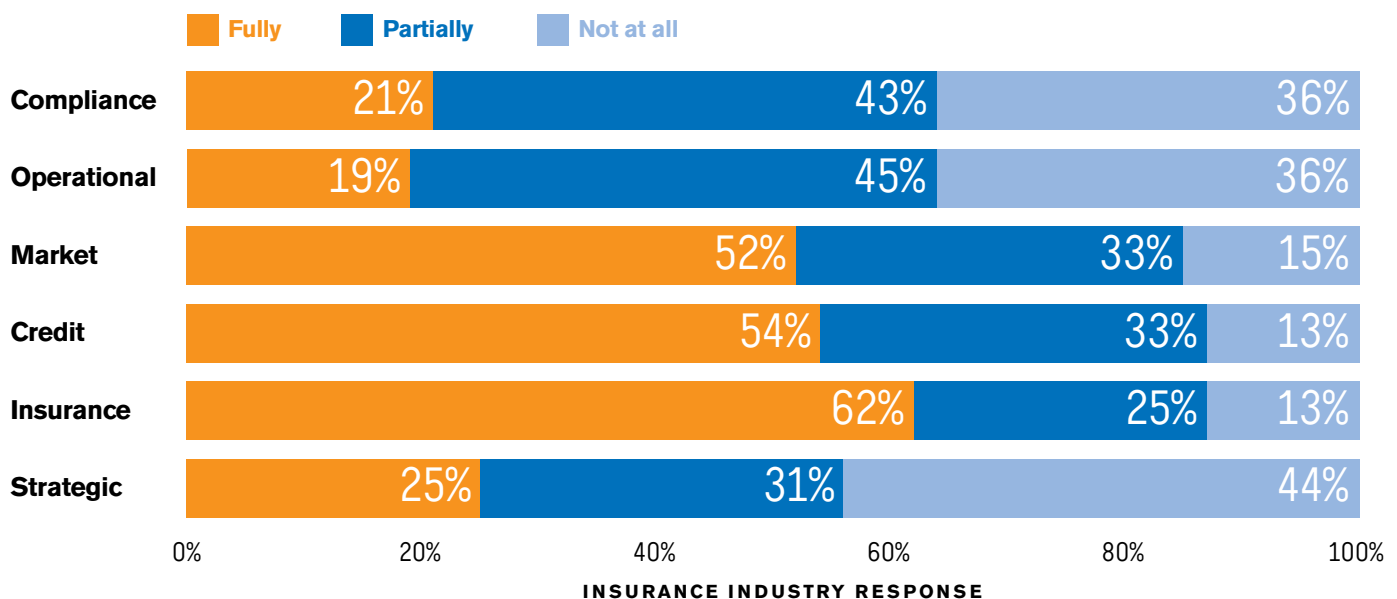
“Ultimately, this lack of integration means that ERM programs may simply be perceived as an additional layer of bureaucracy within the business rather than being integral to how it is run.”

The poor quality of risk data and limited usability of model analysis do not provide a strong basis for decision-making. Less than 40 percent of respondents believe that their risk data and systems are good or excellent. Nearly half believe that their risk information does not support their risk objectives. The survey group saw ERM systems as even less efficient in anticipating emerging risks.

#### Level of ERM Development and Implementation

Survey responses from Insurance Industry

Source: PriceWaterhouse Coopers



## What Is Enterprise Risk Management?

Risk management has increasingly come to be identified with enterprise risk management processes. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) described eight components of ERM systems:

**Internal Environment** The internal environment sets the basis for how risk is viewed, including the risk management philosophy, risk appetite, integrity and ethical values, and the environment in which they operate;

**Objective Setting** Objectives must exist before management can identify potential events that could disrupt their achievement;

**Event Identification** Internal and external events affecting achievement of the objectives must be identified, distinguishing between risks and opportunities;

**Risk Assessment** Risks are analyzed, considering likelihood and impact;

**Risk Response** Management selects risk responses—avoiding, accepting, reducing or sharing risks—and a set of actions to align risks with risk tolerances;

**Control Activities** Policies and procedures are established and implemented to help ensure risk responses are effectively carried out;

**Information and Communication** Relevant information is identified, captured and communicated in a form and time frame that enable people to carry out their responsibilities; and

**Monitoring** The entirety of enterprise risk management is monitored and modifications are made as necessary.

## Five Barriers to an Enterprise View of Risk

Gartner, July 27, 2006

In a survey of 61 business and IT executives operating the retail, energy, financial services, health care and public sector industries, the Gartner Group identified five major roadblocks to ERM:

- Growth trumps risk management as a budgetary priority;
- Risk is subjective—views are siloed and personalized;
- There are multiple, conflicting risk agendas;
- Stakeholders struggle with risk relevance—related both to the success of individual efforts and broader organizational goals; and
- Lack of information is the primary barrier to a transition from silo-based to systems-based risk management.

## Top 10 Enterprise Risk Management Myths

Gordon Burnes, Vice President, Open Pages  
Financial Executive, May 2008

10. **IT Risk Management = Information Security**  
Most information management programs place too much emphasis on the how and what, and far too little on the why. Information risk management is all about why.
9. **CIOs Are Strategically Driving Enterprise GRC Solutions**  
In purchasing compliance platforms, IT is too often at the table in a support role rather than as an advisor on the long-term strategic benefits of a common GRC platform for managing both risk and compliance.
8. **One Size Fits All Approaches Work**  
ERM has to be tailored to an organization's corporate strategies, business activities and external environment; standardized methodologies will likely fail.
7. **Risk Can Only Be Managed from the Center**  
Responsibility for risk management has to be pushed through the organization; accurate information lies at the business line level.
6. **Risk and Compliance Can Be Managed by Spreadsheets**  
Spreadsheets are manually intensive and highly reliant on the individuals who manage the process. Linking, updating and archiving data in spreadsheets is mostly ad hoc.
5. **Traditional Audit Planning Accurately Assesses Risk Factors and Frequency**  
Progressive organizations are turning toward a more agile, top-down approach to risk assessment to drive audit scheduling and frequency.
4. **Enterprise Risk Management Is Dead**  
Today's control-based ERM frameworks have a bias for analysis over action, and the production of documentation sometimes trumps managing risk. ERM should be deployed bottom up, so that business managers are the first-line risk managers.
3. **Risk Management Just Takes Common Sense**  
As business activities have become more complex, so has risk management, which now covers a wide variety of disciplines. It may not be rocket science, but it requires sophisticated models and analytics.
2. **TJX—It Can't Happen Here**  
Preventative technology and knowledge get better every day, but so do the villains. Every organization is susceptible to a breach.
1. **You Cannot Plan for the Unknown**  
Key risk exposures do not always follow a normal distribution. You may not be able to predict them, but you can plan for the events that lie outside the realm of expectations.

## The ERM Approach Is Fundamentally Flawed

### The Board's Neglected Risk Responsibility

David Apgar

Directorship, February 2008

Efforts to market ERM as a brave new discipline have made confusing what was once clear. The manager directly responsible for an operation—be it sales, production, procurement, design or planning—is the best source of information about its risks. ERM can tell you which manager-identified risks the firm can hedge, but it can never discover new ones, such as geopolitical risks that no manager has identified.

Apgar's theory of risk (from his book, *Risk Intelligence: Learning to Manage What We Don't Know*, Harvard Business School Press, 2006) focuses on "learnable" and "random" risks. He maintains that most of the current tool set deals with random risks for which no competitor has an inside track or relative advantage. It is the non-random, learnable risks—involving behaviors, technologies, marketing strategies and supplier relationships—that can put companies at a comparative disadvantage.

For Apgar, the key concept is not just strengthening the capabilities for centralized risk management, but improving the Risk IQ of managers.

- Many (if not all) non-financial risks are learnable: forecasts of customer demand for new products, services and attributes; security and political conditions; the actions of competitors, regulators

and suppliers; capacity and loyalty of workers; creditworthiness of counter-parties; and the effectiveness of new technology.

- While uncertainty underpins all types of risk, managers can differentiate between random risks and learnable risks. Risk assessment tools should evaluate the quality of a business manager's risk information resources, not just the magnitude of the risk. Apgar argues that knowledge about the operating team is the best predictor of how it will handle challenges.

This approach to risk has some key implications for CEOs and boards.

- CEOs and boards should be focused on risk intelligence rather than risk assessment. A company can get into more trouble by selecting risks it is not well-equipped to manage than it can by merely taking on risks that appear large.
- Learnable risks raise competitiveness issues. Random risks do not. This means that an organization might overprotect itself relative to a competitor—or fail to move up the learning curve as fast as its competitor—and create a cost disadvantage for itself. The assumption that worst-case loss depends on only exposure is wrong. It also depends on what is known and who else is taking the risk.
- Boards and CEOs should focus on tools to evaluate the ability of line managers to assess risk.

## The ERM Concepts Are Incomplete—Missing Some Key Components

### Time to Bail on ERM?

Treasury and Risk, June 2008

What is missing in ERM systems are the linkages to corporate strategy. Risk management still has to go from the back room to the board. Specific risks are not always related to strategic risks. (Subprime issues were not even on the radar screen in housing-related industries). Chief risk officers need more than a dotted line reporting to the board or audit committee. There needs to be a clear link between corporate strategy, risk appetite and financial and operational plans. Risk professionals need to have the independence and stature to be able to voice concerns—to close the gap between risk management and business management.

### Integrating Governance, Risk and Reporting to Create Long-Term Value

Brian Ballou and Dan L. Heitger, Strategic Finance, May 1, 2008.

What is missing is an integration of three traditionally disparate topics—corporate governance, enterprise risk management and business reporting. Some organizations structure risk management so that executives who own the process, often titled chief risk officers, report directly to the board. Other organizations structure risk management so that executives who own the process report to the board's risk committee—or even an executive risk committee—on

a nonsystematic basis. A key determination in how organizations implement governance mechanisms to manage risk is the extent to which they have linked risk management to the organization's mission and strategies. Overall, organizations differ greatly in their emphasis. Some emphasize governance if they have prestigious board members who are in high demand. Others emphasize more sophisticated processes for risk management, particularly in regulated industries where they are evaluated on that basis. Organizations that face high levels of media scrutiny typically have more sophisticated processes for monitoring and reporting how effective they are at managing particular risks (death or injury of workers). But very few organizations link their risk management processes to their strategic decision-making processes.

### Issues in integrating corporate governance, risk management and business reporting:

- Assure board oversight of structures to manage risks and report on risk management effectiveness;
- Develop a common risk language across organizational silos;
- Link risk to strategy, creating a portfolio that helps management seek opportunities and mitigate risks where appropriate;
- Implement steps of risk assessment—understanding sources, probabilities, impacts and prioritizing risks within a common framework;
- Respond to risk and understand how choices impact other risks;

- Measure risk responses, residual risk and impact on performance;
- Report risk management information to internal stakeholders;
- Understand external demand for risk management information; and
- Report risk management information to external stakeholders.

### **Marrying Risk and Strategy to Create Value**

Peter Pourquery  
Boston Consulting Group, 2007

In a survey of risk management practices, BCG found that managing risk and formulating strategy remain segregated at a majority of banking institutions. Collaboration between the functions is hampered by organizational structures that calcified years ago, when risk experts were confined to more traditional roles.

Pourquery used a historical example to illustrate his point. In January 1777, General George Washington and Lord Cornwallis gathered their advisors on the eve of battle. Cornwallis presided over a small hierarchical gathering that was described as “less council than court”. Washington’s council was more open and mixed: “Local citizens were invited to attend and speak freely; Washington did not propose a single course of action but framed a problem. Even before a single shot was fired, the outcome was largely decided by how well—or poorly—these leaders tapped their experts, assessed their risks and used that understanding to inform strategy.”

### **Key findings**

- Managers of business lines want their bank’s risk managers to integrate closely with business teams and to act less like internal police and more like strategic advisors;
- More than half of survey respondents would like their risk functions to provide a range of services beyond the traditional purview, contributing to areas such as business strategy and planning and marketing and business development; and
- CRO’s reported that banks continued to exclude risk managers when they convened their own councils of war.

### **Recommendation**

Include risk experts in the development of long-term strategy, for example, by appointing the chief financial officer, the chief risk officer and the head of strategy to a committee charged with exploring strategy within the context of management risk and economic capital.

### **Other Issues that ERM Systems Are Missing Altogether or Not Effectively Addressing**

#### **Reputation and its Risks**

Robert Eccles, Scott Newquist, Roland Schatz  
Harvard Business Review, February 2007

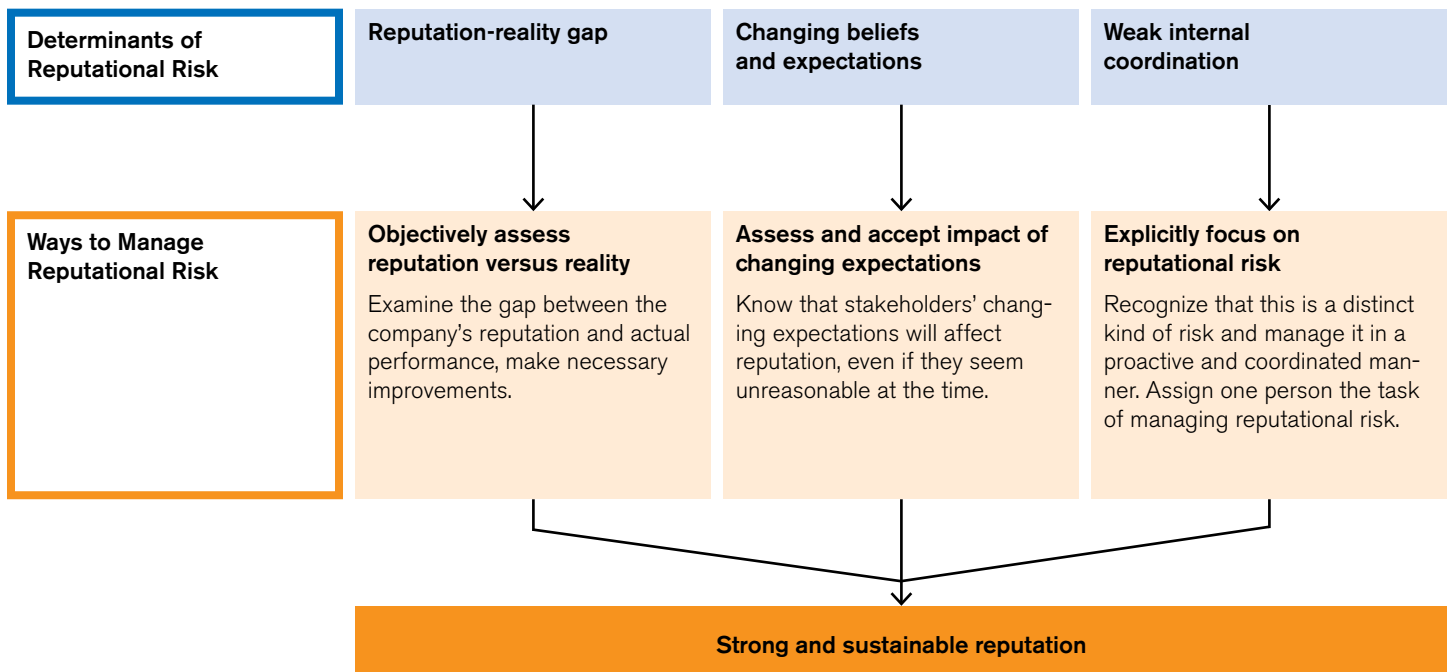
Most companies do an inadequate job of managing the risks to their reputation. The tendency to focus on the threats that have already surfaced is not risk management, but crisis management. When 269 executives were surveyed by the

Economist Intelligence Unit in 2005, 84 percent responded that their CEOs were principally responsible for managing reputational risk—effectively saying that no one manages reputational risk on a day-to-day basis. The authors pointed to three determinants of reputational risk:

- A gap between reputation and reality (e.g. Texas city refinery and Prudhoe Bay problems were at odds with the Beyond Petroleum and due diligence messages);
- Changing beliefs and expectations (GSK suing the South African government for patent infringement on retrovirals); and
- Weak internal coordination among different business units or functions (AMR union wage reductions simultaneous with bonuses for senior managers).

### A Framework for Managing Reputational Risk

Understanding the factors that determine reputational risk enables a company to take actions to address them.  
 Source: Harvard Business Review



### **Navigating in the Midst of More Uncertainty and Risk**

Jim Butcher, Nick Turner, Gerard Drenth  
*Journal of Applied Corporate Finance*, Fall 2006

What is missing is the scenario-building capacity that enables out-of-the-box thinking to anticipate strategic risks. Even as companies are deploying enterprise risk management systems, risks continue to multiply and move into more strategic and macro-event risk arenas. The consequence has been an expansion of traditional risk management tools into realms of greater uncertainty, where managers quickly run up against the limits of quantitative methods and models.

University of Chicago economist Frank Knight distinguishes between risk and uncertainty. Risk applies to cases where the distribution of possible outcomes is either known or can be estimated. Uncertainty is about a potentially unlimited set of choices and a unique situation. Many risks are actually turning out to be “uncertainties” and require new approaches.

The authors describe the use of scenario planning as a valuable tool to navigate between risk and uncertainty, citing four key benefits:

- **Breadth and Diversity of Experience**  
The tyranny of conventional wisdom and uncritically accepted mental models can blind executives to important changes in an industry and macro-environment. One of the real values is to consider the broader context and how it is changing before drawing key business insights;

- **Pattern Recognition**  
Scenario work has the potential to “envision” new patterns that may emerge, rather than simply relying on past patterns;
- **Right Answer, but Wrong Timing**  
A late 1990s scenario about a major financial institution that could not settle was not needed for Y2K, but it created institutional memory and preparedness for a post 9/11 response; and
- **Mental Models and Leadership**  
One of the real accomplishments of scenario planning has been to create more flexibility in executives’ thinking—and a willingness to be more forward-thinking.

### **Stemming the Rising Tide of Supply Chain Risks**

Marsh, April 2008

Nearly three-quarters of the 110 risk managers surveyed say their companies’ supply chain risk levels have increased since 2005—and 71 percent report that the financial impact of supply chain disruptions has also increased—damaging bottom lines, customer retention and brand equity. None of the risk managers surveyed said that their company is highly effective at supply chain risk management today, and just 35 percent said they were moderately effective. Today, the typical risk manager estimates that just 25 percent of his or her company’s end-to-end supply chain is being assessed annually for risk likelihood and impact.

## Under the Spotlight: The Transition of Environmental Risk Management

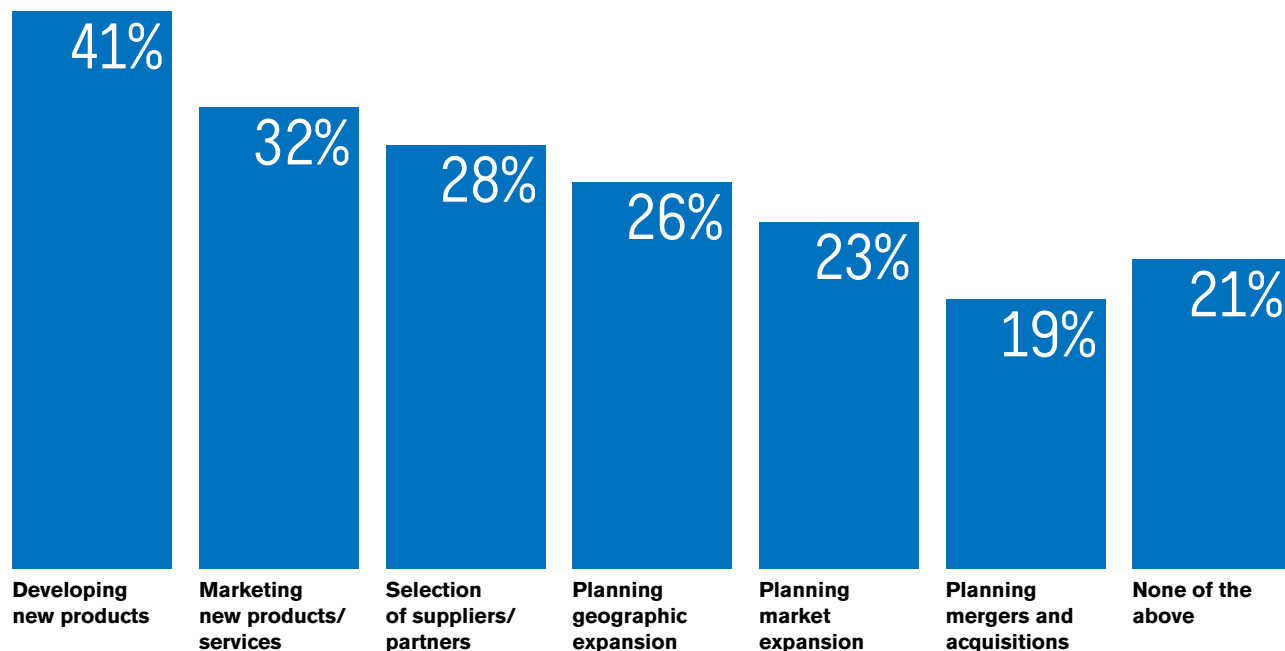
Economist Intelligence Unit, 2008

What is missing is environmental risk management. One-third of companies manage environmental risk in an ad hoc fashion. Another 26 percent manage it in a coordinated way, but without ties to overall risk management. And 10 percent have no management structure for environmental risk.

Survey respondents report that there is no clear consensus about who is responsible for environmental risk. Many companies conduct strategic activities without a formal assessment of environmental risk.

## Formal Consideration of Environmental Risk

Source: Economist Intelligence Unit



## Section 5

# Reaching for Resilience

## Overview

Enterprise resilience represents a new thrust in the effort to anticipate and adapt to turbulence and to assure effective risk management, disaster recovery, business continuity and profitability.

The scientific meaning of resilience refers to the properties of a material to resume an original shape after being bent or stretched. Different authors and organizations have expanded this original focus and definition to preparedness for disruptions large and small: critical infrastructure protection; part of homeland and economic security; sustainability; enterprise risk management; and corporate competitive advantage.

The problem is that the word resilience has so many meanings that it risks becoming meaningless. The Department of Homeland Security uses the term to mean preparedness to recover from catastrophic disruptions, but in practice, homeland resilience tends to look strikingly like homeland security. A number of vendors use the term resilience

**“It’s not the strongest of the species that survives; not the most intelligent... It’s the one that is the most adaptable to change.”**

*Charles Darwin*

interchangeably with IT security, supply chain security, disaster recovery or business continuity.

In Australia, the resilience framework is societal, recognizing interdependence among individuals, organizations and communities. Even the most resilient organization will not be able to meet its goals if the local infrastructure is unable to resume functioning or individuals are not resilient enough to return to normalcy and jobs.

The goal is not just recovery or continuity, but the transformation from reactive to proactive to adaptive—and a set of principles and best practices that enable the transformation.

## Properties of Resilience: The Four Rs

MCEER, University of Buffalo

**Robustness** Strength, or the ability of elements, systems and other units of analysis to withstand a given level of stress or demand without suffering degradation or loss of function.

**Redundancy** The extent to which elements, systems or other units of analysis exist that are substitutable, i.e., capable of satisfying functional requirements in the event of disruption, degradation or loss of function.

**Resourcefulness** The capacity to identify problems, establish priorities and mobilize resources when conditions exist that threaten to disrupt some element, system or other unit of analysis. (Resourcefulness can be further conceptualized as consisting of the ability to supply material—i.e., monetary, physical, technological and informational—and human resources to meet established priorities and achieve goals.)

**Rapidity** The capacity to meet priorities and achieve goals in a timely manner in order to contain losses and avoid future disruption.

## Enterprise Resilience: Managing Risk in the Networked Economy

Starr, Newfrock and Delurey  
Strategy+Business, 2003

During the last half century, the vertically integrated company has given way to the networked enterprise. Successful firms today must deal with intertwined layers of information, raw materials, analytical data, customer communication and service and network infrastructure—at unprecedented speed—while maintaining countless secure relationships with suppliers, technology outsourcers and government regulators.

### Enterprise Resilience (ER) versus Enterprise Risk Management (ERM)

Risk management models have not kept pace with the shift from centralized to networked organizations. Most ERM programs rely on “point solutions,” attempting to moderate risks by “hardening” potentially vulnerable spots. Conventional ERM fails to account for interdependencies across vertical and horizontal operations that characterize the networked world. In contrast, enterprise resilience planning creates an integrated first line of defense and an offensive strategy to guard the entire extended enterprise against new, unavoidable risks that are the byproducts of interdependent operations. Resilience focuses on creating organizations that are “sensing, agile, networked and prepared”, focused on “how to survive before the fact”.

## Redefining the Corporate Governance Agenda: From Risk Management to Enterprise Resilience

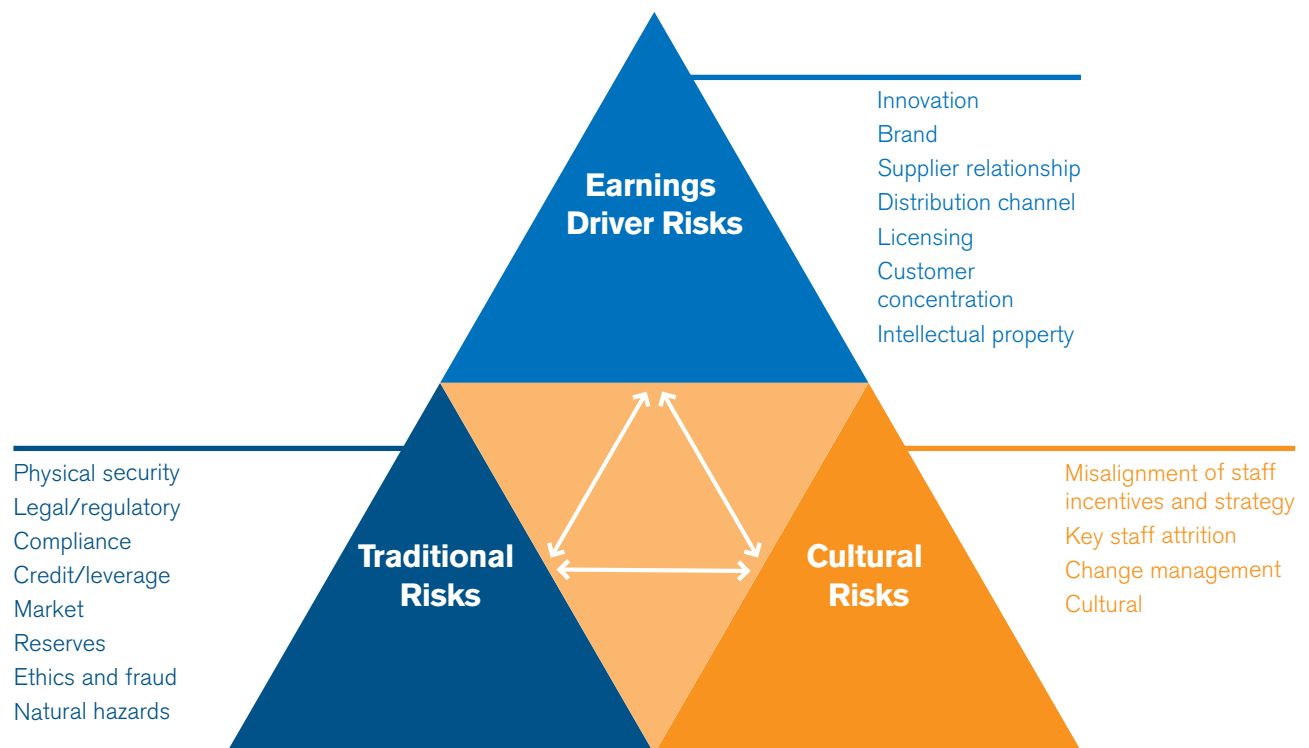
Booz Allen Hamilton & Weil, Gotshal & Manges, 2004

What is missing is the bridge from risk intelligence to enterprise resilience. Traditional risk management systems and solutions are inadequate to handle today's expanded spectrum of market and business risk. As the rate of change in the market accelerates, companies require an adaptive risk management approach that both responds to and anticipates business shifts. Very few companies have managed to develop a dynamic capability for enterprise resilience.

Enterprise resilience is predicated on an expanded view of risk—one that focuses on value and therefore encompasses not only traditional risks (e.g. financial, natural hazard, physical security, legal compliance) but also risks related to earnings drivers (e.g. innovation, intellectual property, partnerships) and company culture. Enterprise resilience marries risk assessment, information reporting and governance processes with strategic and business planning to create an enterprise-wide early warning capability that is embedded in the day-to-day business operations and culture of the firm.

### Enterprise Resilience Expands the View of Risk

Source: Booz Allen Hamilton



## Four Steps to Corporate Resilience

Liisa Valikangas  
Strategy+Business, 2004

The author argues against the conventional wisdom that corporate failure and death are essential to economic health, and questions the logic that start-ups can replace the wisdom and wealth accumulated by a more mature company. Rather than survival of the fittest, a truly healthy approach to economic adaptation and wealth creation is for companies to become more resilient.

Four ways that companies can build the capacity to continually renew themselves include:

### Rethink Underlying Principles of Management Decision-Making

Managing a resilient corporation requires a greater willingness to access information from multiple sources and to avoid guidance by those with a vested interest in the status quo;

### Generate a Portfolio of Strategic Options

Resilient companies build a portfolio of experimental strategies from all parts of the company. Some portion of capital expenditures—30 percent or so—should be earmarked to test new strategies and innovate aspects of the company business model;

### Careful Examination of Resource Allocation

Most companies create budgets based on a legacy principle: if you have been successful, you deserve funds in the future. A more resilient solution is to manage resources so that funding for known opportunities is balanced by an appetite for new ventures; and

### Implement More Effective Corporate Governance

Directors have to make sure that management has a plan for the future that does not just relive the past but provides the right resources to promote resilience.

## Living on the Frontline: The Resilient Organization

KPMG Business Continuity Centre of Excellence, 2007

In the evolution toward “the resilient organization”, there are three mutually dependent challenges: People, Diversity and Coordination.

### People Come First. Five focus areas include:

1. Accounting for people immediately after a disaster;
2. Effective communication with staff and family members through the recovery process;
3. Developing a clear understanding of where corporate and individual responsibilities lie in various scenarios;
4. Developing a better understanding of the human impact of major disasters; and
5. Increasing flexibility through cross-training in order to resource “spikes” in demand.

### Diversity of Solution. Three key aspects highlighted:

1. Greater use of remote working capabilities;
2. Setting up split-site operations for larger-scale critical functions; and
3. Enabling the transfer of critical operations to other global locations without depending on significant staffing from the affected location (moving the work, not the people).

### Coordination with the Public and Private Sectors.

#### Key issues include:

1. Sharing experience with other firms;
2. Anticipating planning for supply chain disruptions;
3. Regular communication with regulators, civil authorities and emergency services; and
4. Participation in market-wide exercises and benchmarking activities.

## The Resilient Enterprise

Yossi Sheffi  
MIT Press, 2005

Companies are now exposed to a multitude of unexpected events—from natural disasters such as earthquakes to terrorist attacks and supplier failures. They not only need to become more resilient to these shocks, but they can actually increase their everyday competitiveness and gain strength from such disruptions.

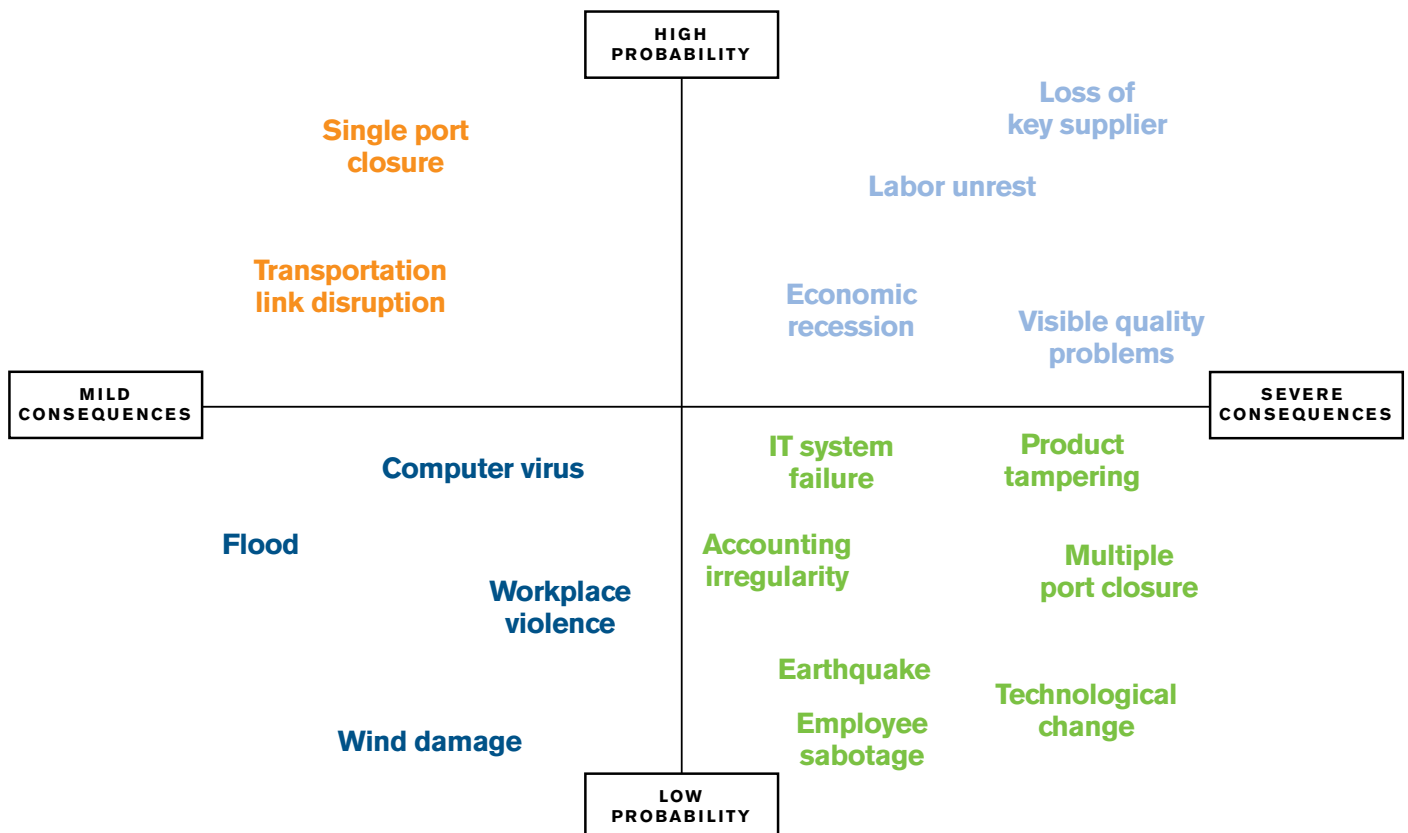
A company can become more resilient by designing its supply chain for robustness. One of the standard ways is to use redundancy, which is expensive. Other ways to make the system more resilient include: forging strong relationships with critical suppliers while developing alternatives for

commodity suppliers; working with interchangeable parts; cross-training employees; deploying flexible manufacturing; utilizing concurrent processes of design, manufacturing and distribution; delaying product differentiation downstream in the supply chain so products remain in a fungible state as long as possible; and collaborating with trading partners.

These principles create supply chains that are not only resilient but also flexible and that can respond to day-to-day demand changes. One begets the other, because a supply shortage and a demand spike are, at their core, a problem of supply/demand mismatch. Companies that have built their supply chains to respond to significant demand fluctuations have also built in the ability to respond to supply shortages.

## Enterprise Vulnerability Map

Source: The Resilient Enterprise, Yossi Sheffi, MIT Press, 2005



## Relationships, Layoffs and Organizational Resilience

Gitell, Cameron and Lim  
University of Michigan, September 2005

Resilience in everyday parlance refers to the capability to 'absorb strain and maintain coherence' (Oxford English Dictionary). In organizational science, it refers to A) the maintenance of positive adjustment under challenging conditions, B) the ability to bounce back from untoward events, and C) the capacity to maintain desirable functions and outcomes in the midst of strain. Resilience is a dynamic capacity of organizational adaptability that grows and develops over time. It is not a static attribute that organizations do or do not possess. Rather, it results from processes that help organizations retain resources in a form sufficiently flexible, storable, convertible and malleable to avert maladaptive tendencies and cope positively with the unexpected.

The authors argue that organizational resilience is akin to individual resilience in one key way: resilience grows out of the cohesiveness with a group. They argue that the two key characteristics of resilience are a strong commitment to employees (relational reserves) and the financial resources to maintain those commitments in the face of unanticipated events.

In a study of 10 major airlines after 9/11, the authors demonstrated a negative correlation between the extent of employee layoffs and the recovery of share value during a subsequent three year period. Firms that had announced the largest layoffs recovered less of their stock value, which the authors attributed to the loss of relational reserves between companies and their employees.

They also noted that, although a lack of financial reserves makes an organization vulnerable to crisis and more dependent on layoffs as a coping strat-

egy (and therefore less resilient), Wall Street tends to discourage high levels of financial reserves as a poor use of capital. The example cited was Southwest Airlines, which:

- Laid off no employees and had the fastest stock price recovery;
- Was able to weather the storm because of its strong financial reserves; but
- Southwest's conservative approach had been criticized by Wall Street analysts who argued that the airline should use its extra cash to make acquisitions or buy back stock.

## Organizational Resilience

Robert Oldfield, 2007

In an attempt to manage a turbulent environment, most organizations have mature risk, business continuity, security and emergency management programs. Unfortunately, these programs frequently manage turbulence in isolation from each other. Risk managers maintain risk registers. Security managers conduct threat and vulnerability assessments and business continuity managers carry business impact analyses. A resilient organization recognizes the synergies between these functions. It recognizes that a risk is a risk regardless of whether or not it has been identified and regardless of who identifies it.

Resilience is not a plan or a checklist. The elements of a resilient organization are:

- **Adaptive Capacity**  
Recovery to an original state may not be the best option, and organizations need to be able to adapt to maintain competitive advantage;
- **Communications**  
Lack of communications has been a contributor to global disasters when those who had the information did not pass it on, or when those in authority did not act on it;

- **Interdependencies**  
Independent thinking is not suited to interdependent reality. Independent people who do not have the maturity to think and act interdependently may be good producers, but they will not be good leaders or team players;
- **Situational Awareness**  
Awareness includes understanding risks and vulnerabilities, enabling quick detection of change and rapid response;
- **Leadership**  
The key elements include principle-centered leadership, non-hierarchical communications and empowerment to act;
- **Culture and Values**  
Culture is about how principles are learned and translated in day-to-day behavior. Values contribute to the culture and may include integrity, customer focus and results;
- **Enterprise-Wide**  
All business units and functions contribute to organizational resilience; and
- **Ownership**  
Resilience is not a word to describe only one of the tactical elements of security, risk or business continuity. It is the balanced integration of all of these.

### **Business Resilience**

The ability to rapidly adapt and respond to risk and opportunities in order to maintain continuity of business operations, remain a trusted partner and enable growth.

### **Business Resilience for the Global Marketplace: Transforming Operating Risk Into Competitive Advantage**

Jet, June 2008

In pursuit of global competitiveness, organizations no longer operate within one country or region. Instead they rely upon a network of partners to build, review, transport or otherwise deliver a better, less expensive, faster-to-market product or service than they could on their own. The lure of the global marketplace is a double-edged sword; there are costs to adequately managing new risks and disruptions.

The tools and processes of risk management have evolved from reactive to proactive to adaptive.

### **Disaster Recovery**

Incident management and disaster recovery initiatives tend to answer the “what if” question. They focus on quick response to disruption: insurance (to transfer risk and pay for recovery); incident reporting (to learn about disruption quickly); and response

plans and response services (to provide aid to people and operations in need). Disaster recovery tends to be reactive in nature.

### Business Continuity

Business continuity experts answer the question: “When” our business is disrupted, how will we continue to provide service to our customers? Organizations utilize real-time intelligence, business continuity plans and decision support technology and services to guide fast decisions about what to do next. Business continuity tends to be proactive in nature.

### Business Resiliency

Resilience asks how to gain competitive advantage from managing risk. Resilient organizations use predictive intelligence for early warning and situational analysis and historic intelligence to identify and seize new opportunities. They leverage a common operating platform across departments and business units for a global perspective. They routinely communicate with employees, partners and customers. Resilient organizations are adaptive.

### Business Resiliency: Moving the Mountain an Inch at a Time

Mary Herbst, May 2008

Mary Herbst, director of business resiliency, described the “Road to Resilience” for Carlson Hotels. Back in 2004, there was no clearly defined plan for business continuity. Accountability was an IT function, not a business function. Plans were written for audit purposes, not for implementation. And, technology planning was scattered and non-specific.

### Business Resiliency Model

Source: Mary Herbst



### Attributes of a Business Resiliency Program

- Comprehensive
- Well-coordinated
- Integrated
- Measured
- Well-supported
- Funded

During the next two years, risk management processes began to be formalized. Accountability moved from IT to audit business risk management. Technology plans were completed, risk assessments performed, specific governance resources assigned to each operating group, and disaster recovery planning coordinated with business continuity.

Hurricanes Katrina and Wilma dispelled complacency about readiness plans, while the threat of a pandemic triggered a renewed commitment to transform business continuity into business resilience.

- **The Resiliency Goal**  
Protection of people, assets and brands through planning, risk analysis, risk mitigation, crisis response and the continuity of business and technology.
- **Critical Ingredients for Success**  
Executive support, operating group ownership, funding, business resiliency councils, strong partnerships, change management processes and the integration of business resiliency into all aspects of the business.

#### Lessons

- Integrating Business Resiliency in all areas of the business ensures that resources are ready to respond to all critical events;
- Without executive sponsorship, all efforts will dissipate;
- It is a long and winding road;
- There are no “silver bullets”;

- It takes commitment from the top and resources from all levels of the organization; and
- When you feel like giving up—remember “why” it is so critical.

#### **National Organizational Resilience Framework Workshop**

Australia, December 2007

Australia has begun considering how critical infrastructure protection can evolve into a next generation approach, like resilience.

The words “critical infrastructure protection” create misconceptions in four ways. Critical infrastructure protection is perceived to be:

- Focused on asset protection rather than service delivery;
- Associated with security rather than the continuity of systems;
- Limited to protection of assets rather than a partnership with the emergency management community; and
- Focused on terrorism rather than all disruptions.

Resilience is neither a plan nor a checklist. The capacity is found in an organization's culture, attitudes and values. A resilient organization:

- Is adaptive and can work with or in spite of uncertainty;
- Puts change and adaptation in its vision;
- Foresees the future and acts on it;

### **Question CEOs Should Ask**

What are our key vulnerabilities?

What are our critical interdependencies?

How do we monitor for new threats and incorporate them into our risk practices?

What strategic changes are occurring in our threat environment?

Who would be our leadership team in times of crisis?

How do we ensure all business units work in a united way during a crisis?

How should we ensure all of our staff are informed of our immediate priorities in a crisis?

Do we have a program ready to build and maintain staff morale during response and recovery to a crisis?

Are mutual aid agreements in place with our sector peers?

Which key stakeholders would support us in times of adversity? Which would attempt to undermine us?

- Ensures staff know what to do;
- Understands its interdependencies;
- Makes and seizes opportunity in times of crisis;
- Values the resilience of the community within which it operates;
- Thinks outside the box; and
- Capitalizes on adversity and change.

## America the Resilient

Stephen Flynn

Foreign Affairs, March-April 2008

The United States is becoming a brittle nation. When the power goes out, Americans are incapacitated. Two decades of taxpayer rebellion have stripped down emergency preparedness capabilities. Most public health and emergency management departments are not funded adequately to handle routine work. Aging infrastructure compounds the risk of destruction and disruption. One of the rationales for building the interstate highway system was to support the evacuation of major cities if the Cold War turned hot. In 2006, the year the system turned 50, Americans spent a total of 3.5 billion hours stuck in traffic.

What Washington should do, instead of sounding the alarm about apocalyptic terrorist groups, is arm Americans with greater confidence in their ability to prepare for and recover from terrorist strikes and disasters of all types. Such resilience results from a sustained commitment to four factors.

### 1. Robustness

The ability to stay standing in the face of distance. Robustness entails good design, redundancy or substitutability, and investment in good maintenance.

### 2. Resourcefulness

Skillfully managing a disaster once it unfolds. Identifying options and prioritizing what should be done to control damage and to begin mitigating it.

### 3. Rapid Recovery

Resume operations as quickly as possible.

### 4. Review

Learn and make changes, capture strategic advantages.

Over the past two decades, we have stopped thinking about the elements of our physical infrastructure as national security assets. In fact, increasingly it seems that we have stopped thinking about infrastructure altogether. Many of the great public works projects of the 20th century—dams and canal locks, bridges and tunnels, aquifers and aqueducts, and even the Eisenhower interstate highway system—are now old and are not aging gracefully. There are real costs associated with our neglect...When critical systems become unreliable, businesses have to invest in backup capabilities to sustain their operations. Over time, this can weaken the competitive position of companies in the international marketplace. Alternatively, a national effort to repair and upgrade these systems would bolster the attraction of investing, working and living in the United States. Company supply chains would be more efficient and reliable. Corporations could channel some of their investments in continuity-of-operations contingencies back into their core businesses. Insurance costs would be reduced.

Stephen Flynn

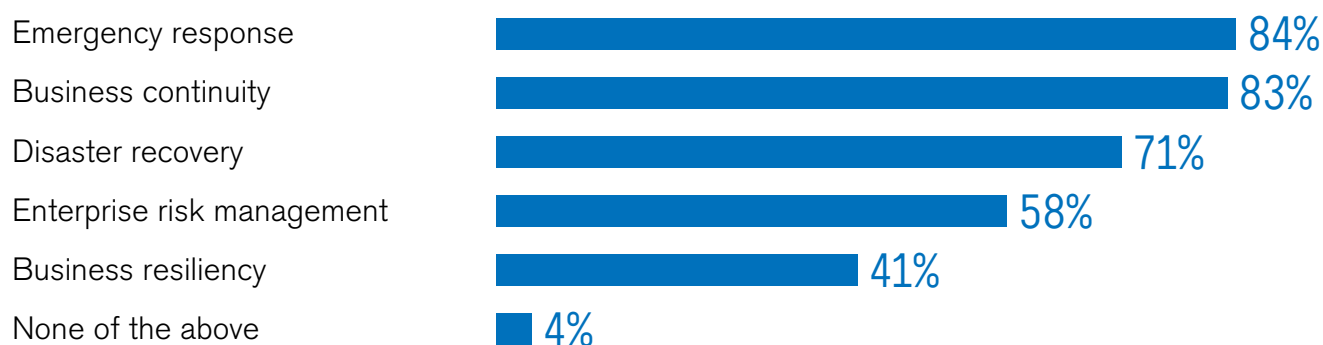
*The Edge of Disaster: Rebuilding a Resilient Nation.*

## 2008 Business Resiliency Survey Results

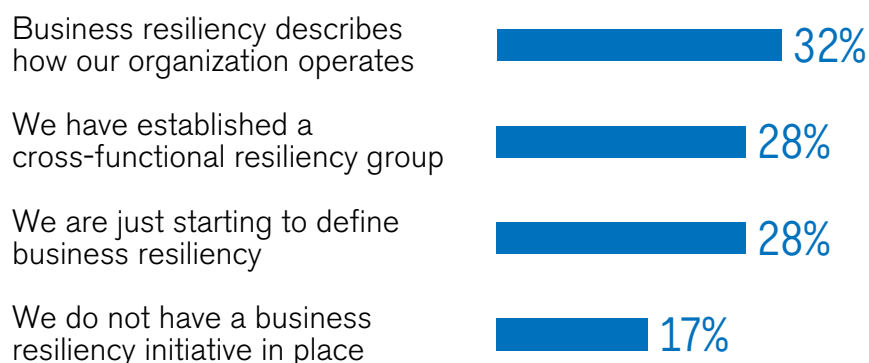
An Insider's Look at the Current State of Risk Management, Continuity and Resiliency in Multinational Organizations

Source: IJet

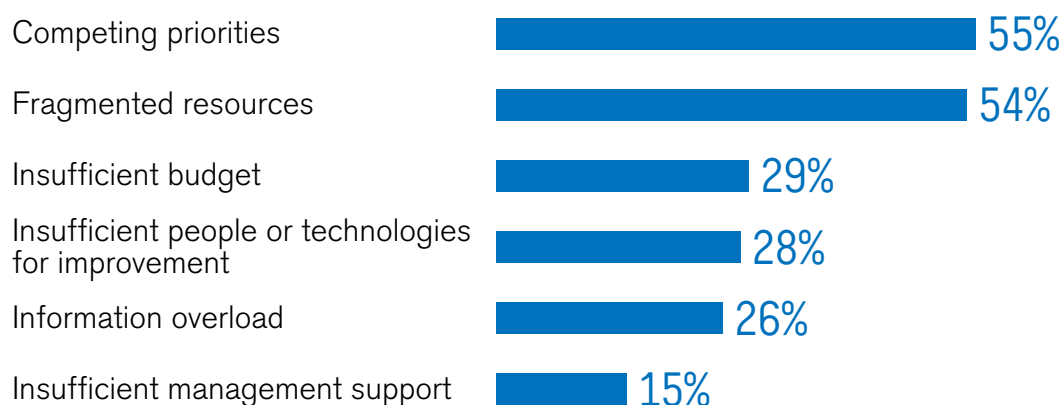
### What types of plans does your organization have in place?



### How would you describe your organization's approach to business resiliency?



### What are the top barriers to instituting stronger risk management, continuity and resiliency plans?



## Section 6

# Roles for Governance

**“Management is doing things right; leadership is doing the right things.”**

*Peter F. Drucker*

**“The only alternative to risk management is crisis management.”**

*James Lamm*

## Overview

Some key surveys and studies find that directors are “in the dark” when it comes to risk management. There is general agreement that non-financial risks are poorly measured, that organizational structures for managing risk are inadequate and that boards need to take a more hands-on role in overseeing risk management processes. But there is currently no agreement on what exactly that role should be.

In the majority of companies, audit committees have primary responsibility for risk management, but they are being overwhelmed as non-financial risks (with financial reporting implications) are added to their plates. Some studies see a danger in Balkanizing risk. Others see a problem with the creation of a risk committee, which can give other board committees the perception that risk is no longer their problem.

One area that is emerging (but even less evolved) is the potential role of the audit committee to oversee internal and external audits of financial and non-financial risk management processes and to evaluate the validity of management risk rankings.

### ***In the Dark: What Boards and Executives Don't Know About the Health of Their Businesses***

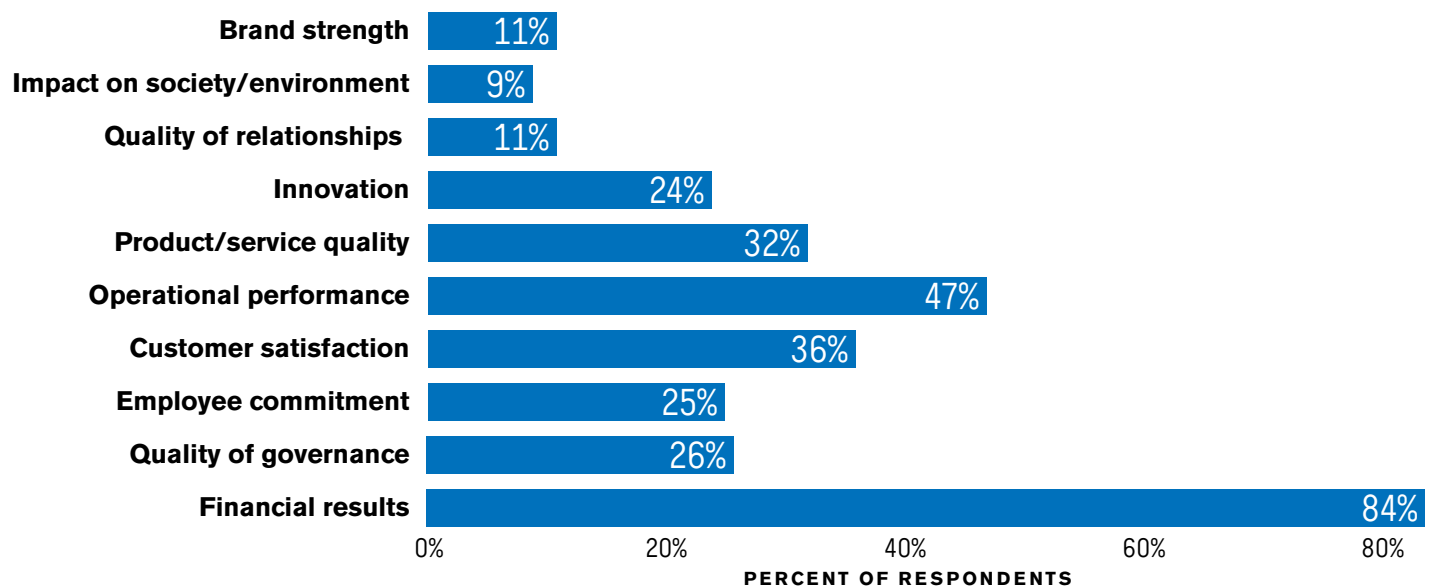
Deloitte and Economist Intelligence Unit, 2004

In a survey of 250 executives and board members, Deloitte found that the two largest barriers to effective risk governance systems were a lack of tools needed to analyze non-financial issues and a culture of skepticism that such non-financial indicators are directly related to the bottom line.

- Nearly three-quarters of executives and board directors were under pressure to measure non-financial performance indicators.
- One-third of respondents said their companies' non-financial reporting measures were excellent or good (versus an 86 percent positive response rate for financial reporting measures).
- Nearly half of respondents said non-financial reporting measures were ineffective or highly ineffective in shaping the decision-making process.

### **Areas in Which Board Holds Management Accountable and Offers Rewards for Good Performance**

Source: Deloitte, *In the Dark II*



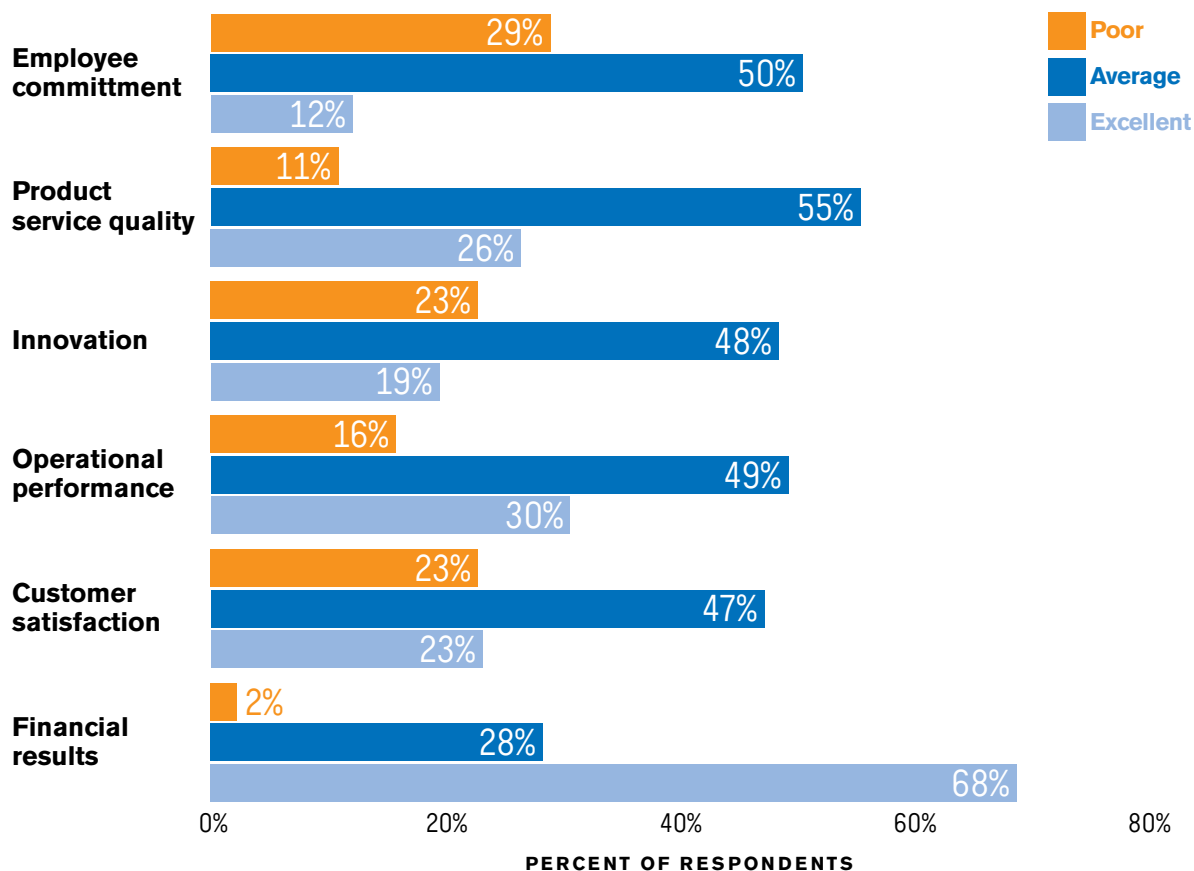
## ***In the Dark II: What Boards and Executives Still Don't Know About the Health of Their Businesses***

Deloitte and Economic Intelligence Unit, 2007

Three years later, the results were re-tested. The majority of executives perceived a growing need to better understand the underlying drivers of their performances through non-financial measurements. But, the metrics available to monitor performance remained inadequate. The study concluded that companies either did not have or were not sharing critical non-financial performance data with their boards.

### **Quality of Information Shared with the Board**

Source: Deloitte, *In the Dark II*, 2007



## Taking Risk on Board

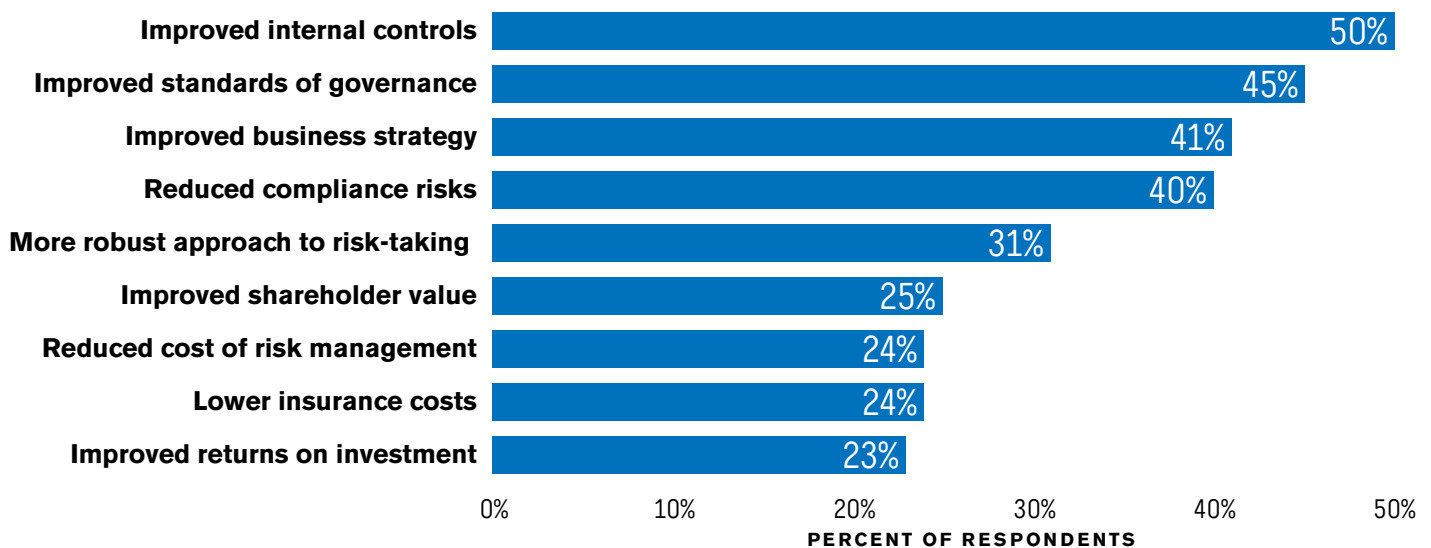
Lloyd's with the Economist Intelligence Unit, 2005

Boards are taking risk more seriously. Three years ago, just one in ten boards spent more than 10 percent of their time on formal risk management. By 2005, that number had risen to almost 40 percent. Yet, this change has not translated into greater expertise.

In the 12 months prior to the survey, one in five companies surveyed had suffered significant damage from a failure to manage risk and more than half (56 percent) had experienced at least one near miss. Ten percent of respondents reported three near misses during the past year. Adoption of risk management standards across the enterprise was limited. Only one-quarter set regular risk targets for managers, and fewer than one-third provided risk management training for managers and staff. This was viewed as symptomatic of a culture in which risk management was considered to be "someone else's job."

## Positive Results Following Increased Board Responsibility for Risk Management

Source: Economist Intelligence Unit



## The Risk Intelligent Board: Viewing the World Through Risk-Colored Glasses

Steve Wagner and Maureen Errity  
Deloitte.com, Winter 2008

To meet their fiduciary responsibilities, directors must share a common vision of risk and adopt a framework to support their risk oversight activities. Unfortunately, these elements are lacking at many companies.

This is not to imply that boards are negligent when it comes to risk. Most board members make careful deliberations and bring to bear their best judgment. They summon the chief risk, strategy and audit executives along with the external auditor and others who manage exposures to risk. They listen to presentations, ask tough questions and review reports.

What is lacking is a context for understanding the issues. The board has nothing to benchmark against; directors have no processes or frameworks in place

that allow them to take independent, objective views. As a result, they are left grappling with risk on an almost intuitive level, an ad hoc approach that allows issues to slip through the cracks.

Creating a risk committee is no panacea. In fact, it can be counterproductive if other board committees believe that their risk problems are solved because the risk committee is on the job.

When the risk management structure is optimized, every board committee will have risk on its agenda. Financial risk falls within the domain of the audit committee; compensation risk, the compensation committee; and succession risk, the nominating committee. Each of these committees, in turn, reports back to the full board, which processes the information to develop a full-spectrum picture of risk. And the loop is closed when the full board addresses risk issues with management on a regular basis.

## Two Faces of Risk

Steve Wagner and Mark Layton  
Deloitte.com

We call the two faces of risk “rewarded risk” and “unrewarded risk”.

Unrewarded risk represents what poker players call “table stakes”: you’ve got to ante up just to get into the game. For instance, every public company in the United States must comply with payroll tax withholding laws, observe OSHA health and safety requirements and pay bills when they come due. Yet companies that perform all of these tasks in a timely and competent manner don’t see their share prices surge as a result. The primary incentive for addressing these risks is value protection, not value creation.

Conversely, rewarded risk represents the strategic bets that you place during your poker game. You’ve assessed your hand, sussed out the competition and wagered a stack of chips with the expectation of raking in many more than you’ve laid out. In business, rewarded risks are those bets you make as you develop new products, enter new markets or acquire new companies. The primary motivation for taking rewarded risks is to spur value creation.

Fixate on just one side of the coin and you’ll get a one-sided result. Focus on value creation (rewarded risk) to the exclusion of value protection (unrewarded risk), and you’ll quickly find yourself on the slippery slope of noncompliance, litigation, reputation risk and other nastiness. Similarly, address only unrewarded risk and ignore rewarded risk, and your company may survive but will never thrive.

## Global Warming: The Director's Perspective

Kevin A. Ewing

NACD-*Directors Monthly*, August 2008

Global warming presents corporate risk of the most challenging kind—dynamic, long-range and multivariable. The board's responsibility with respect to global warming is one of oversight of the executive team's efforts. Four key tasks emerge:

- **Test**  
Boards should continually validate the adequacy of the executive governance program;
- **Communicate**  
Global warming reaches into many facets of a company's operating and strategic plans and can play a cameo role in numerous presentations. Boards should consider whether these disaggregated communications will suffice;
- **Advise**  
Board members can, often more easily than management, import insights gained from outside sources; and
- **Align**  
Boards are uniquely positioned to observe the degree of alignment between the governance model being applied to global warming-related corporate risks and the strategic decision-making process as a whole.

The key is to define the oversight responsibilities of the board in relation to the responsibilities of the executive team, using traditional notions of oversight and governance to drive a disciplined corporate strategy on a complex issue.

## Audit Committee Member Survey 2007-2008

KPMG

A survey of nearly 300 audit committee members of public companies revealed:

- Nine out of ten say that the audit committee has been more effective since the passage of Sarbanes-Oxley; members are confident about their oversight of "traditional financial reporting matters";
- Over half of audit committee members believe that their effectiveness is hampered by overloaded agendas, compliance activities that can detract from substantive discussion of issues and inadequate communication and coordination with the board and other standing committees; and
- Risk management is the No. 1 priority of the audit committee members, but only 28 percent are satisfied that the audit committee understands management's processes to identify and assess significant business risks. Only 21 percent are very satisfied with the information and reports they receive from management.

## The Role of U.S. Corporate Boards in Enterprise Risk Management

Carolyn Kay Brancato, Matteo Tonello and Ellen Hexter, with Katharine Rose Newman  
Conference Board, 2006

Key findings from the survey included:

- An increasing number of directors acknowledge that they must oversee business risk as part of their strategy-setting role. Nevertheless, most board members tend to resist excessive formalization of risk oversight processes;
- Directors believe that strategic risk rather than financial risk is their key concern;
- Most directors say they have a good or very good grasp of the risk implications of strategy, but are less likely to appreciate how the different parts of a business interact in the overall risk portfolio;

- Less than half of directors can point to the robust techniques that help them oversee risk (e.g. risk ranking), and the majority of boards do not use a ranking system as part of the risk assessment practices;
- Two-thirds of companies currently delegate risk oversight to their audit committees; and
- In 23 percent of companies, another committee shares the responsibility with the audit committee. A few, mostly financial, institutions have established separate risk committees (16 percent in the financial services area versus less than 4 percent in the non-financial services area).

A theme in the survey and interview data is that company-wide risks are too complex for the audit committee to manage exclusively, and that identifying a separate committee apart from the audit committee would most likely result in a more robust system of identifying and assessing risk management issues.

The study identifies a potential risk management structure, which can coordinate between committees principally responsible for risk and the full board. (See Governance Structure for Risk Management chart on the following page.)

### **Oversight of Risk Management: Considering the Audit Committee's Role and Responsibilities**

KPMG, Audit Committee Newsletter, June 2007

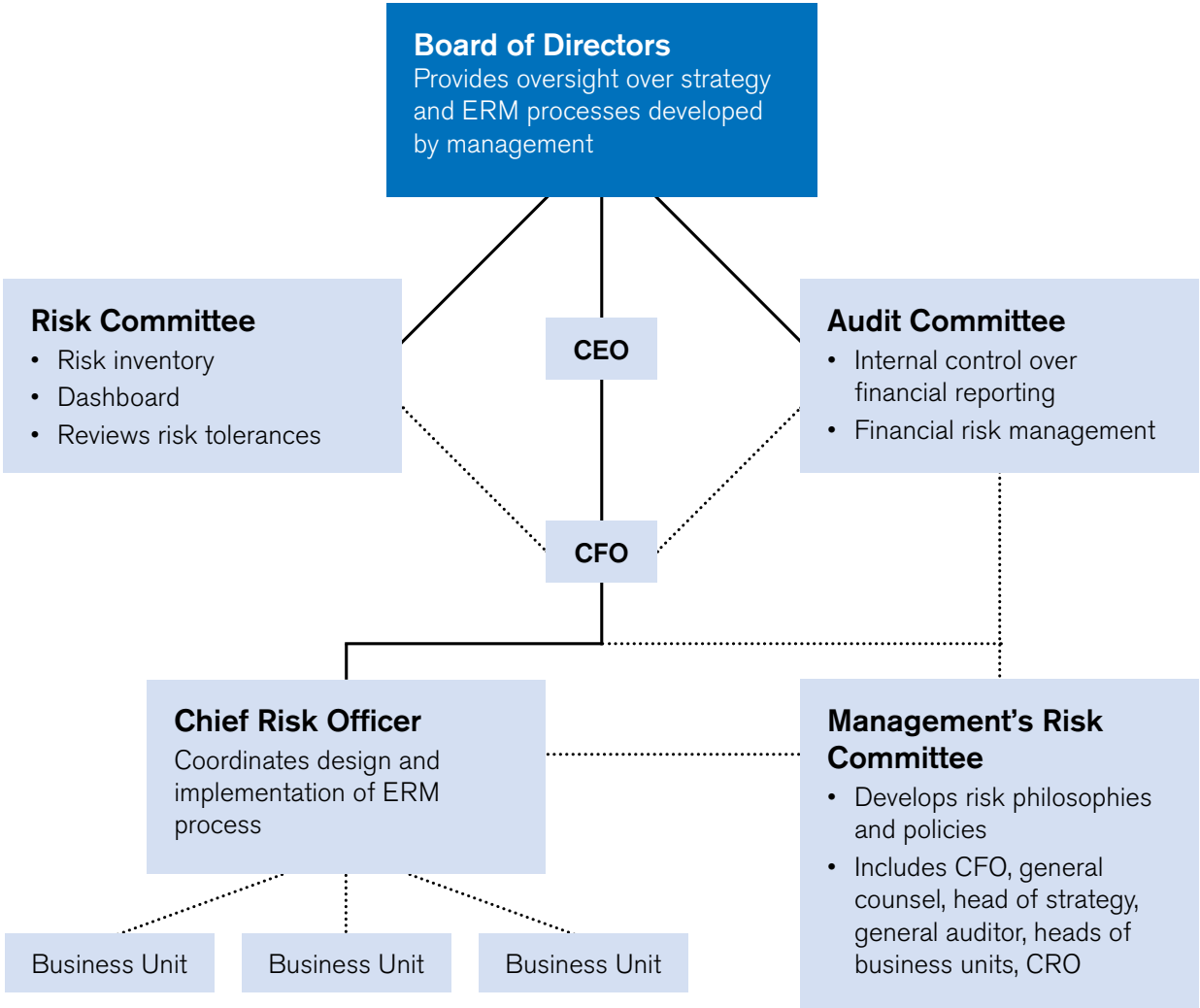
The oversight of risk—by audit committees, boards and other board committees—is evolving and typically lacks a clear delineation of oversight roles and responsibilities. There is no bright line that delineates oversight roles and responsibilities. On the other hand, while a committee structure can provide “specialized oversight”, it may also lead to Balkanization of risk oversight activities as well as gaps in oversight.

An important role for the audit committee is to help ensure that the internal and external audit plans properly focus on internal risk controls. The audit committee should consider whether the internal and external auditors have:

- Communicated their processes for identifying and ranking the financial and non-financial reporting risks they believe may have financial reporting implications;
- Focused their audits on key areas of risk and ensured that procedures are appropriate given the potential impact and occurrence of significant risks;
- Identified the same risks that management identified, and explained any variations from identified risks or risk rankings; and
- Communicated the design and performance of planned audit procedures and demonstrated that the procedures are responsive to identified risks.

### Governance Structure for Risk Management

Source: Conference Board



Section 7

# Recommendations for Risk Intelligence and Resilience

## Overview

Much less has been written on a systems approach to creating the culture and incentive structures that reward effective risk management and resilience. There are at least three major areas to explore: management and governance; the “market movers,” including ratings, insurance and audit industries; and the government by fiat, exhortation or incentive.

## Roles for Management and Governance

### Viewing Risk Management Strategically

Risk and Insurance Management Society, Inc. and Marsh, 2008

Strategic risk management incorporates all of the areas from traditional and progressive approaches, but adds the C-suite view of the totality of risk. The practitioner of strategic risk management views risk as something to optimize, not just to mitigate or avoid, by taking an enterprise-wide view of risk and using it to increase the company’s competitive advantage. Risk is indexed against the organization itself, year after year, and against competitors. And risk management information systems and other technologies play a large role in managing risk.

### Moving from Traditional to Strategic Risk Management

Source: RIMS and Marsh

Traditional Risk Management	Progressive + Traditional Risk Management	Strategic + Progressive + Traditional Risk Management
<ul style="list-style-type: none"> <li>• Risk identification</li> <li>• Loss control</li> <li>• Claims analysis</li> <li>• Insurance and risk transfer methods</li> </ul>	<ul style="list-style-type: none"> <li>• Alternative risk financing</li> <li>• Business continuity</li> <li>• Total cost of risk</li> <li>• Education and communication</li> </ul>	<ul style="list-style-type: none"> <li>• Enterprise-wide risk management</li> <li>• Indexing of risk</li> <li>• Use of technology</li> </ul>

Ultimately, the effectiveness of the enterprise risk management system will depend on the commitment of the CEO and board to implement processes that are tailored to the organization. As Rick Funston of Deloitte observes: “One size fits one.”

### ERM Strategies: The Good, the Bad and the Innovative

Tom Hettinger, Risk and Insurance, September 15, 2008

Companies are adopting three key strategies to manage risk on an enterprise basis:

- A risk identification mindset that pervades the company so that everyone is tuned to identify problems that could interfere with achievement of goals;
- A risk communications strategy that enables employees to share information that will uncover emerging risk possibilities; and
- Use of computer modeling and simulation to understand varying magnitudes of risk and to integrate risk information across business units and geographies.

### Putting Risk in the Comfort Zone

Deloitte Research, September 2008

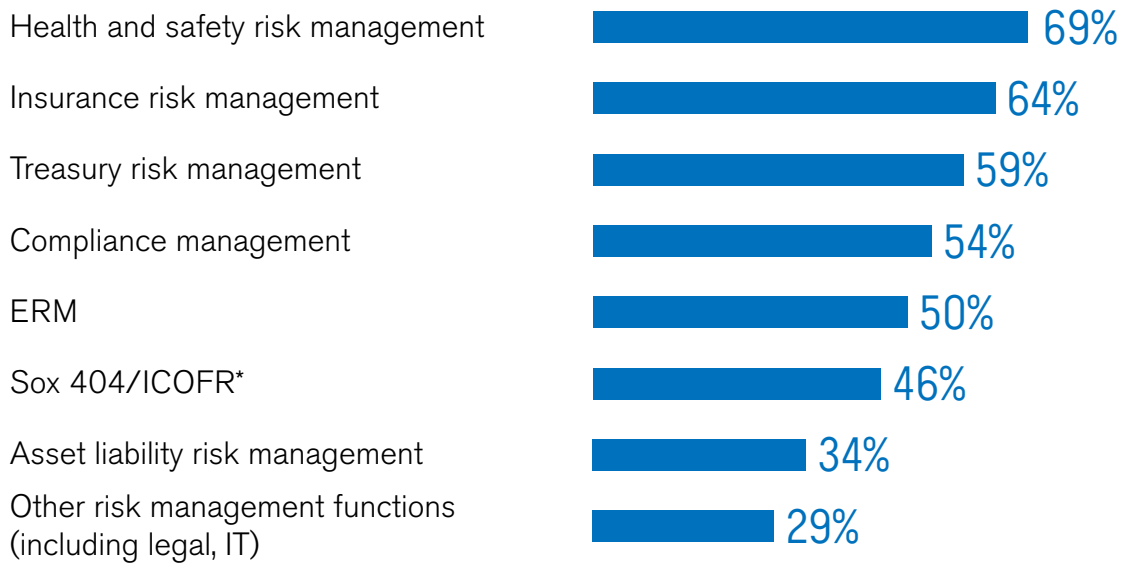
Deloitte has identified nine principles for enterprise risk intelligence. Successful companies will:

- Create a common definition for value preservation and creation;
- Establish a common risk framework supported by appropriate standards;
- Define and delineate key roles, responsibilities and authorities;
- Create a common risk management infrastructure;
- Require transparency and visibility of risk management practices for governing bodies (boards, audit committees);
- Ensure that executive management oversees design, implementation and maintenance of risk program;
- Give business units responsibility for performance and management of risk within the risk framework;
- Ensure that key functions (finance, legal, HR, tax, IT) are not only risk owners, but also support business units in risk management; and
- Have key oversight functions (audit, compliance, risk management) provide objective assurance on the effectiveness of the risk program.

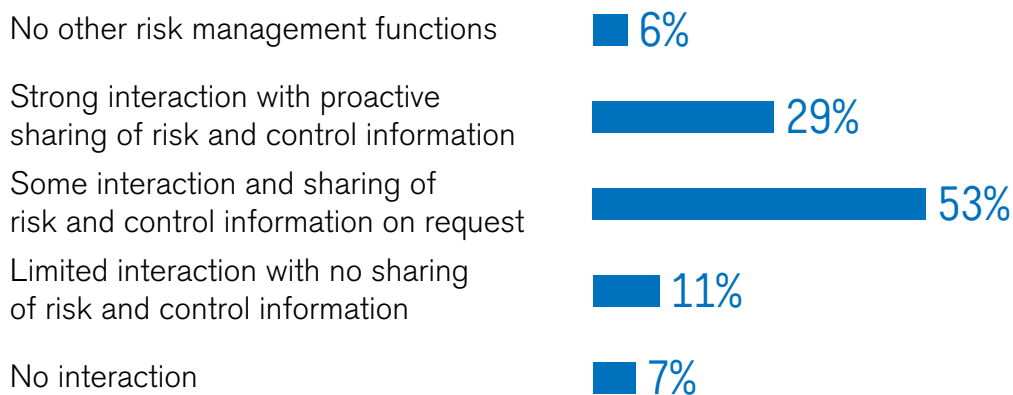
## Global Internal Audit Survey

Source: Ernst & Young, 2007

### Companies Have Multiple Risk Management Functions...



### ...but Levels of Interaction Are Low



\*ICOFR = Internal Controls Over Financial Reporting

### Who Needs ERM?

John J. Hampton, *Business Insurance*, July 14, 2008

Who needs enterprise risk management (ERM)? My answer is, at least four people within an organization: the chief executive officer, the chief financial officer, the internal auditor and the risk manager.

If ERM means listing the 2,000 to 3,000 or so risks that face an organization, no one really needs it. An undisciplined approach to identifying risk and integrating risk mitigation into a single program will bog down after much expenditure of time and money. On the other hand, a disciplined ERM structure is just what is needed by the CEO, CFO, auditor and risk manager, among others.

The CEO and CFO seek transparency and accountability. The Sarbanes-Oxley Act requires the CEO and CFO of public companies to verify internal controls and reliability of financial statements. Rating agencies require risk programs to achieve favorable ratings on debt issues. The internal auditor is responsible for monitoring compliance with company policies and directives. The risk manager needs to present exposure to insurers and others as part of risk management and the purchase of liability coverage.

**“The typical business school today is concerned with business functions, not management...The trouble with the emphasis on analysis is that it leads to an emphasis on technique or formula thinking...something that can be used in place of a brain. Technique has a place in management, but it must be used carefully and in context...not as a way of compensating for lack of experience.”**

*Henry Mintzberg*

## Room for Improvement

### Risks of Complacency

*Towers Perrin Study Showed Business Leaders Appeared Confident in Ability to Manage Risk As Credit Crisis Loomed, Business Wire, March 13, 2008*

The study showed that nine out of 10 executives believed they were as good as or better than their industry peers in managing risk and opportunity. The banking industry was the most confident about its ability to manage operational and strategic risk, and second only to the insurance industry about managing financial risk.

The study included 69 insurance industry participants, each of which was rated by S&P in terms of the firm's ERM capability—weak, adequate, strong or excellent. As part of the study, each firm's response was correlated against its S&P ERM rating. Companies with “excellent” S&P ERM ratings tended to be more risk conservative. For example, only 14 percent of the “excellent” firms were more willing to accept risk than their industry peers, versus 31 percent of other companies. These “excellent” companies also tended to be less confident about their ability to manage all risks and opportunities.

### Economic Capital Models: Working Well?

*Risk and Insurance, September 1, 2007*

Solvency II has spurred European companies to spend a lot of time on the quantification end of risk management. They are now beginning to implement their internal economic capital models, which better reflect the value of the entire enterprise as well as valuing liabilities on a capital market basis. They are also restating their balance sheets. As they do so, some insurers are finding that, in meeting their statutory requirements, they are actually overcapitalized on an economic or capital-market valuation basis. During the first quarter of 2007, AIG says it conducted a preliminary analysis of firm-wide economic capital requirements. That analysis showed that by year end 2006, AIG had excess capital in the range of \$15 billion to \$20 billion.

### Diffusing Risk Through Derivatives?

*Risk: Keeping Ahead of the Curve, Federal Reserve Bank of Chicago, July 2008*

Research shows that the aggregate use of derivative instruments—in particular rate options, interest rate futures and interest rate forwards—is associated with higher growth rates in consumer and industrial loans. Engaging in derivative activities allows banks to lessen their systematic exposure to changes in interest rates, so they can increase their lending activities without increasing total risk. It is uncertain how much banks use credit derivatives to manage risk and whether their credit derivatives positions reduce or increase systematic risk.

## Roles for the Market Movers

Why don't the markets value resilience? If these are bet-the-company risks, how do analysts make buy recommendations without knowing how the company manages risk or its resilience to turbulence? With insured losses on the line, why doesn't the insurance industry play a larger role in creating a premium for resilience? Why doesn't the audit industry identify ways of verifying non-financial claims of companies? The following articles explore ways in which these market movers are beginning to move the markets.

### S&P ERM Questions

Steven Dreyer, S&P Managing Director, September 2008

- How are key risks identified, updated and dealt with?
- How is risk tolerance defined and communicated?
- Who "owns" risk in the organization, and how is success measured?
- What is the board's involvement in risk management?
- How did your company respond to \_\_\_\_\_ ?

## 1. RATINGS AGENCIES

### Enterprise Risk Management: S&P To Apply Enterprise Risk Analysis To Corporate Ratings

S&P, May 7, 2008

The ratings agency announced that it will begin to incorporate ERM into discussions with rated companies in the third quarter and begin to include commentary in ratings reports in the fourth quarter. Its proposal identifies four major analytic components:

- Firm-specific risk management culture and governance;
- Existing risk controls;
- Emerging risk preparation; and
- Strategic risk management.

A firm whose ERM program is considered weak will be missing complete controls for one or more significant risks and will have limited capabilities to identify, measure and comprehensively manage risk exposures. A firm whose ERM program is considered adequate will exhibit conventional "silo-based" risk management processes, in which risks within its business functions are well-managed, but its risk responses are not well-coordinated across business units. A company whose ERM program is rated strong will exhibit an enterprise-wide view of risks allowing for consistent identification, measurement and management of risks across business units within predetermined risk tolerances. The company will also include risk and risk management discussions in its strategic business planning efforts.

A firm rated as excellent will, in addition to those characteristics of strongly-rated companies, also exhibit risk/reward optimization behavior.

The ERM analysis will emphasize risk management culture and strategic risk management. Risk management culture includes:

- Risk-management frameworks or structures currently in use;
- Clear and defined roles for staff responsible for risk management and reporting lines;
- Internal and external risk-management communications;
- Broad risk-management policies and metrics for successful risk management; and
- The influence of risk management on budgeting and management compensation.

Strategic risk management includes:

- Management's view of the most consequential risks the firm faces, their likelihood and the potential effect on credit;
- The frequency and nature of updating the identification of these top risks;
- The influence of risk sensitivity on liability management and financing decisions; and
- The role of risk management in strategic decision making.

### **S&P Rolls Out ERM Review**

John Cummings, *Business Finance*, May 13, 2008  
businessfinancemag.com

S&P is not the only ratings agency pushing ERM. Moody's has been developing a holistic risk management rating methodology through its Enhanced Analysis Initiative. AM Best has stated that ERM will be included as an integral part of its rating process, though not as a separate rating factor.

The S&P model focuses on risk management culture and strategic risk management.

## **2. INSURANCE**

### **The Risk Landscape of the Future**

Swiss Re, 2004

The chief prerequisite for successful risk management is readiness to address highly unsettling questions. What would happen if the Gulf Stream were to lose strength or suddenly change course? What would it mean if nanoparticles actually penetrated the human brain directly via the olfactory nerve? What risks are created by the broad rejection of genetically modified food? The immediate purpose of discussing such scenarios is to differentiate between the possible and the impossible. In reality, the public debate about risks of the future is often dominated by equally irresponsible scaremongering and trivializing reassurance, both of which hamper any attempt at rational risk management.

Risk reduction is too often limited to efforts at reducing the probability of occurrence, not the magnitude of risk.

The world has become demonstrably safer. Since 1970, life expectancies have risen, and the number of fires and traffic accidents has declined. But despite fewer accidents, there are much higher losses per incident.

- In aviation, the number of accidents per one million takeoffs fell dramatically, but the number of fatalities per accident has doubled, and will go higher still with the introduction of 800-passenger planes.
- In rail, state of the art safety has reduced the probability of accidents, but high speed trains magnify the possible consequences as a doubling of speed means a quadrupling of the force of collision impact.
- Urban areas are growing vertically. More traffic and shopping centers are being relocated underground and, worldwide, there are 37 residential blocks higher than 200 meters and dozens more on the drawing board. Escape routes are getting longer and fires can have devastating consequences.
- Increasing dependence on power and telecommunications for economic activity has increased the potential for multibillion dollar productivity losses.

For simple linear systems, loss events can be predicted precisely if all cause and effect relationships

are known. That is why it is possible to calculate how many hours an aircraft propeller can operate before becoming critically warped through the centrifugal forces that cause the metal molecules to migrate gradually to the tips of the propeller blades. For complex systems, accurate predictions are extremely difficult. The real difficulty of risk assessment does not lie in a complex system per se, but in the acceleration of changes in complex systems.

### **Disaster Risk Financing: Reducing the Burden on Public Budgets**

Swiss Re, June 2008

Natural catastrophes are a growing certainty and a rising burden. In 2005, economic losses from natural catastrophes hit a record high, with direct financial losses of \$230 billion (0.5 percent of total worldwide GDP). Despite a record insurance payout of more than \$83 billion, uninsured direct losses of \$150 billion had to be carried by individuals, companies and the public sector. More recently, in 2007, a total of 335 natural catastrophes led to losses of \$64 billion across the globe, of which \$40 billion were uninsured.

Events such as flooding, storms and heat waves place a huge burden on the public sector, which not only carries the cost of relief efforts but is also responsible for rebuilding public infrastructure. This is intensified by the fact that public entities consciously or unconsciously decide to retain risk by not insuring their infrastructure.

Although developed countries typically account for the majority of economic losses, the burden in terms of GDP is dramatically higher for developing countries. In Turkey, a single earthquake caused an economic loss of 11 percent of GDP. In the absence of widespread insurance coverage, economic losses of this magnitude can only be addressed with significant public sector or relief funding.

Traditionally, the public sector has adopted a post-event approach to disaster funding, including increasing taxes, reallocating funds from other budget items, accessing domestic and international credit and borrowing from multilateral financial institutions. Most rely on assistance from international aid.

Pursuing a post-disaster strategy has several potential disadvantages, including: diverting funds from key development projects to pay for emergency relief; paying the premium to raise new domestic debt in a credit constrained post-event market; and raising taxes which could weaken the economy further and discourage new private investments. Finally, international aid often arrives too late for immediate disaster relief.

There is value in shifting from relief to pre-event risk financing, i.e. setting up financial reserves, contingent debt agreements, insurance and alternative risk transfer solutions.

A new generation of sovereign insurance can make it easier for governments to cope with disaster. One example is the GlobeCat securitization. Launched

### **What is a Catastrophe Bond?**

In essence, investors place funds in a catastrophe bond and, if a catastrophe occurs that “triggers” the bond, (each bond has a unique trigger mechanism), investors may lose some or all of the capital investment. In the case of an event, the funds are paid to the bond sponsor—an insurer, a reinsurer or corporation—to cover losses. In turn, the bond sponsors pay interest to investors for this catastrophe protection. Catastrophe bonds offer investors an attractive risk/return profile and serve to diversify portfolio risk.

*Swiss Re*

in 2007, this solution uses financial instruments to transfer Central American earthquake risks to the capital markets. GlobeCat provides a payout based on the size of the population exposed to a specified earthquake above a threshold level. Three events of \$150 million are covered in a three year period. Of this total amount, \$160 million was placed in the capital markets through a catastrophe bond (that defined magnitude, location and depth) and the remainder was reinsured.

### **Crediting Preparedness**

Raisch and Statler, Intercep, NYU, 2006

#### **Apply the preparedness standard for pricing risk.**

The authors suggest that specific inclusion of corporate preparedness in rating and underwriting processes could deliver shareholder value. Property insurer FM Global takes the position that business interruption insurance is the last line of defense against business disruption, while the first and most important step is a holistic risk management program that includes all aspects of the facility and operation. The insurer proves the bottom-line benefits of its position by comparing the loss history of policy-holders that had implemented its loss prevention approach to those that had not.

On balance, preparedness yielded 75 percent to 85 percent lower dollar losses. For Hurricane Katrina, FM Global clients collectively spent \$2.3 million to prevent losses that were estimated at \$480 million. In other words, for every dollar spent on targeted preparedness measures, \$208 were saved in one single major event.

### **3. AUDIT**

#### **The Future of Corporate Sustainability Reporting**

Brian Ballou, Dan Heitger and Charles Landes

*Journal of Accountancy*, December 2006

#### **Create standards for non-financial reporting areas.**

Using corporate sustainability reporting as an example, the authors show how audits can play an important role in non-financial reporting areas. Increasingly, social and environmental performance has become an important issue for internal and external stakeholders. A survey of investors, portfolio managers and securities analysts reported that 90 percent of those questioned said annual reports should go beyond financial and shareholder issues to include environmental sustainability and corporate governance. The most dominant reporting regulations come from the Global Reporting Initiative (GRI), which issued its first comprehensive reporting guidelines in 2002 and the G3 Reporting Framework in October 2006. As of October 2006, more than 1,000 international companies had registered with the GRI.

Although many firms have affiliated themselves with GRI standards in their corporate social responsibility reporting (CSRs), there are no commonly accepted criteria for audits of these reports. The authors conclude that as demand for reporting on corporate social responsibility and sustainability grows, so too will the role of accountants and auditors to verify the accuracy of reported information. And this may open the door to address other stakeholder demands for information on non-financial performance, such as risk management and governance.

## The Right Fit: Auditing ERM Frameworks

Alexandra Psica, *Internal Auditor*, April 2008

An ERM framework is not a single policy, but an array of components within an organization that work together to manage risk over time efficiently and effectively. The auditor's task is to assess whether the sum of these components constitute a framework that is appropriate for the organization.

### Establishing a Framework

Auditors should focus on the attitudes and values described in the organization's risk management policies and governance frameworks. Although auditors are not involved in establishing the framework, when they conduct an audit, they should look for evidence that the risk management practices defined in the framework are in use and operating as expected.

### Assessing Risks

Auditors should check to see if the organization has a consistent risk identification process that addresses all categories of risk in its business environment. They should determine whether there is a formal risk assessment process, whether residual risk exposure

is examined against established risk tolerances and whether a formal response to risk is documented and communicated.

### Treating Risks

Auditors should look for action plans to manage unacceptable risks, including specific mitigation measures, time lines and owners. Key risk indicators should be identified and monitored on a regular basis by those responsible within the organization. Auditors should check for a standardized approach to managing risk information with common language and data.

### Monitoring the Framework

An organization should have processes and practices that enable it to monitor the effectiveness of the ERM framework. Auditors should look for pre-established objectives and indicators that the ERM processes and framework are measured against. Auditors should assess whether there is both management oversight of the framework to ensure that the processes are working as intended and independent oversight to monitor the quality of risk management and due diligence in risk decision making.

## Internal Audit Role in ERM

Source: *The role of internal audit in enterprise-wide risk management*, (power point), James Glass, director, Business Review and Audit Division, Financial Services Authority, United Kingdom

### Core risk-based internal audit roles

- Giving assurance on the risk management processes
- Giving assurance that risks are correctly classified
- Evaluating risk management processes
- Evaluating reporting of key risks
- Reviewing the management of key risks

### Legitimate internal audit roles with safeguards

- Giving advice on identifying and classifying risks
- Championing establishment of ERM
- Facilitating risk workshops
- Facilitating management's response to risk
- Central coordinating point for ERM
- Monitoring risks across the business
- Holistic reporting on risks
- Developing risk management strategy for board approval
- Operating the ERM framework

### Roles internal audit should not undertake

- Imposing risk management processes
- Managing risks on management's behalf
- Setting risk appetite
- Taking decisions on risk responses
- Accountability for risk management
- Management assurance on risks

## Global Internal Audit

Ernst & Young, 2007

Do internal audit functions have the resources to refresh annual risk assessments?

- Eighty-nine percent of respondents conduct a risk assessment to support the internal audit planning process.
- Forty-four percent of respondents update their risk assessment semi-annually, quarterly, or prior to conducting internal audits.
- Only 44 percent of respondents provide standardized training to individuals responsible for conducting a risk assessment.
- Only 43 percent of respondents present risks not covered by the internal audit plan to the audit committee.
- Only 21 percent of respondents were able to complete the prior year internal audit plan.
- Only 24 percent completed up to 80 percent of the plan.

## Roles for Government Policy

Government policies can reinforce the private sector by incentivizing investments, strengthening market mechanisms that reward resilience, creating resilience standards for government contracts to leverage its own buying power, investing in risk analytic tools and computational models that improve risk assessment capabilities and information-sharing networks, and leveraging public-private partnerships that identify needs and encourage joint solutions.

### Transform

Debra van Opstal, Council on Competitiveness, June 2007

The national objective is not just protection but resilience—the ability to bounce back. And the mission is not just homeland security, but economic security—the ability to resume operations and take advantage of new opportunities.

To create a more resilient economy, the government should:

### Lead By Incentive

- Leverage the government's buying clout to embed resilience criteria into procurement processes and supply chains;
- Leverage the government's investments in technology to embed resilience criteria into the evaluation and selection of emerging technologies;
- Leverage market incentives more creatively; and
- Expand guidance on disclosure of non-financial material risks in SEC filings.

### Create More Effective Partnerships that Reduce Cost and Risk

- Fund additional research to apply computational modeling and simulation capabilities to risk assessments;
- Create regional networks to exchange information on infrastructure or system risk management, crisis planning and preparedness, non-proprietary best practices and intelligence-sharing between the public and private sectors; and
- Expand the program of technology test beds that help companies test innovative security solutions without interrupting or endangering current operating systems.

### Education and Training: Change the Culture

- Establish a resilience curriculum fund to which universities or other education/training providers can apply for funding to develop programs—either stand-alone or modules embedded into existing curricula; and
- Stimulate cross-disciplinary research that creates new capabilities for understanding complex systems, interactions and interdependencies.

### Homeland Security 3.0

Heyman and Carafano, The Heritage Foundation and CSIS, September 18, 2008

Major areas of recommendation include: empowering a national culture of preparedness; shifting to a resilience-based strategy; expanding international cooperation throughout homeland security programs; developing a framework for domestic intelligence; and establishing national programs to improve professional development in security and public safety. With respect to risk and resilience, the report recommends that the federal government:

- Allocate financial support and other federal resources on a risk basis, not on fixed percentages. The federal government should highlight best practices, and develop and promote baseline community preparedness capabilities standards. The federal government should develop a basic risk assessment to enable communities to evaluate relative risks realistically.
- Establish a model that delineates governmental and private sector roles and responsibilities. Defeating terrorists is not the private sector's job. Government should be clear on what it expects from the private sector, as well as:
  - Define what is reasonable through clear processes and performance measures;
  - Create transparency and the means to measure performance;
  - Provide legal protections to encourage information sharing and initiative; and

A country risk officer, comparable to the role of a chief risk officer, is a useful model to develop an integrated perspective across the social, economic and environmental risks of a country. The country risk officer would take the lead in creating a national risk landscape, promoting the common understanding and forward-looking dialogue essential for risk prevention and adaptation measures.

*Peter Forstmoser, Swiss Re*

- Tailor expectations to the unique characteristics of each sector.
- Propose and fund an investment strategy to facilitate public-private partnerships more effectively, target national transportation trust funds by creating an independent infrastructure fund, encourage joint investment in border infrastructure, transfer federal trust funds back to the states, and focus investments on project-based financing.
- Develop leadership on global and national resiliency issues. The term “critical infrastructure” has often been used in a sloppy and overly-inclusive manner, lumping “critical” and “dangerous” into one concept. Critical assets need to be made more resilient through greater redundancy, robustness and/or decentralization, while dangerous facilities must be protected against attack.

### **Top Ten Challenges for the Next Secretary of Homeland Security**

Homeland Security Advisory Council, September 11, 2008

1. Recognize that “homeland security” is more than a single Cabinet department.
2. Inventory DHS’s commitments, deadlines and work with Congress to create a rational oversight system.
3. Improve intelligence and information sharing.
4. Build a cadre of homeland security leadership through a unified system of training and education.
5. Build the R&D and acquisition process to support DHS missions.
6. Complete the work of strengthening national disaster response capabilities.
7. Lead the building of a resilient America with a:
  - Nationwide application of a “resilience metric”—time to reconstitution of everyday services;
  - All-hazards approach; and
  - Active engagement of private sector and academic sector thought leaders.
8. Balance secure borders and open doors to travelers, students and commerce.
9. Take the following steps to improve risk management and risk communications:
  - Improve risk-based approach to homeland security;
  - Establish and improve performance metrics for measuring risk and build a framework for risk-informed decision-making;
  - Consolidate existing risk management programs across components and agencies; and
  - Improve risk and crisis communications systems.
10. Improve sustainability of national homeland security efforts by strengthening the financial base and the urgency of mission focus.

### **Partnering With the Private Sector to Secure Critical Infrastructure**

William G. Raisch, Testimony

House Homeland Security Committee, May 14, 2008

Implement legislation passed in 2007 that calls for the development of a voluntary private sector certification program for all-hazards emergency preparedness.

Government should consistently engage the private sector in the development and implementation of the program, maintain an integrated approach across relevant offices and functions, provide sustaining resources to the program, evaluate the voluntary application of the program to critical infrastructure, and help to develop education and tools to enable businesses to pursue program assessment and implementation with minimal cost and disruption.

## **Building a Resilient Nation: Enhancing Security, Ensuring a Strong Economy**

Reform Institute, October 2008

A truly resilient nation places equal emphasis on preparedness, protection, response and recovery so that it can withstand disruptive events that it knows are inevitable irrespective of their origin.

- The next administration and Congress must refocus the nation's homeland security policy with resilience at its core.
- DHS needs to be a national resource—a clearinghouse—charged with:
  - Conducting an extensive public awareness campaign targeting U.S. industry and empha-sizing the criticality of workable business continuity plans;
  - Assisting U.S. industry in developing business continuity plans by providing templates, advice, best practices and general “help desk” like services; and
  - Taking a leadership role in the development and implementation of national, regional and local exercises with private sector interests focused on testing business continuity plans.
- Congress and the next administration need to refocus DHS and its customs and border protection agents on working with the private sector to more effectively identify potential threats to the global supply chain, specifically in the adoption of more effective screening technologies and deployment of “smart containers”.

### **Neglected Defense**

Flynn and Prieto, Council on Foreign Relations, March 2006

There are three reasons why relying on the market as the primary catalyst for critical infrastructure protection is flawed. First, security is a public good and core responsibility of government. Second, by relegating itself to “protector of last resort”, Washington ends up taking a wait-and-see approach that delays the pursuit of practical security measures. Third, if private sector preparedness is simply assumed, the only way to validate that the private sector is prepared is after an attack.

To make America more secure:

- Washington needs to change its policy paradigm, which in effect tells companies to protect themselves;
- Washington must move beyond talking about information sharing with the private sector and hold government officials accountable for actually doing it;
- Congress and the administration should work closely with industry to establish security standards and implement and enforce regulations where necessary, and especially where industry is seeking standards and regulation;
- Congress should establish targeted tax incentives to promote investments in security and resiliency in the highest risk industries;
- Congress should establish federal liability protections for companies that undertake meaningful security improvements;
- Private sector assets and capabilities should be fully integrated into more frequent exercises to respond to catastrophic events; and
- DHS should establish a federal awards program, modeled after the Baldrige Quality Award, which recognizes private sector achievement and innovation in homeland security.

## Council on Competitiveness

### BOARD

#### Chairman

Charles O. Holliday, Jr.  
DuPont

#### University Vice Chairman

Shirley Ann Jackson  
Rensselaer Polytechnic Institute

#### Labor Vice Chairman

Douglas J. McCarron  
United Brotherhood of Carpenters and  
Joiners of America

#### Chairman Emeritus

F. Duane Ackerman  
BellSouth Corporation

#### President

Deborah L. Wince-Smith

### EXECUTIVE COMMITTEE

Gene D. Block  
University of California, Los Angeles

Erskine B. Bowles  
The University of North Carolina

William R. Brody  
The Johns Hopkins University

Jean-Lou A. Chameau  
California Institute of Technology

Richard T. Clark  
Merck & Co., Inc.

Jared L. Cohon  
Carnegie Mellon University

John J. DeGioia  
Georgetown University

John M. Engler  
National Association of Manufacturers

Marye Anne Fox  
University of California, San Diego

James Hagedorn  
The Scotts Miracle-Gro Company

Sheryl Handler  
Ab Initio

John L. Hennessy  
Stanford University

John A. Hillerich IV  
Hillerich & Bradsby Co., Inc.

Susan Hockfield  
Massachusetts Institute of Technology

Steven Knapp  
The George Washington University

D. Michael Langford  
Utility Workers Union of America, AFL-CIO

Richard T. McCormack  
Merrill Lynch & Co., Inc.

Edward J. McElroy  
American Federation of Teachers, AFL-CIO

Samuel J. Palmisano  
IBM Corporation

Ralph R. Peterson  
CH2M HILL

James M. Phillips  
Pinnacle Investments

Michael E. Porter  
Harvard University

Luis M. Proenza  
The University of Akron

James H. Quigley  
Deloitte Touche Tohmatsu

Ian C. Read  
Pfizer Inc

Kenan Sahin  
TIAX LLC

David E. Shaw  
D. E. Shaw Research

Lawrence Weber  
W2 Group Inc.

Robert J. Zimmer  
The University of Chicago

## Council Membership

### GENERAL MEMBERSHIP

Michael F. Adams  
The University of Georgia

Anthony J. Alexander  
FirstEnergy Corporation

Robert A. Altenkirch  
New Jersey Institute of Technology

Craig R. Barrett  
Intel Corporation

Thomas R. Baruch  
CMEA Ventures

Alain J.P. Belda  
Alcoa, Inc.

Robert J. Birgeneau  
University of California, Berkeley

Lee C. Bollinger  
Columbia University

Richard H. Brodhead  
Duke University

Amber M. Brookman  
Brookwood Companies Incorporated

David L. Callender  
The University of Texas, Medical Branch  
at Galveston

George Campbell, Jr.  
The Cooper Union for the Advancement  
of Science and Art

Judith Cardenas  
Lansing Community College

Curtis R. Carlson  
SRI International

David F. Carney  
Lincoln Educational Services

John T. Casteen, III  
University of Virginia

Clarence P. Cazalot, Jr.  
Marathon Oil Corporation

Thomas A. Cellucci  
Department of Homeland Security

Roy A. Church  
Lorain County Community College

Mary Sue Coleman  
University of Michigan

France A. Córdova  
Purdue University

Michael M. Crow  
Arizona State University

Ruth A. David  
Analytic Services, Inc. (ANSER)

William W. Destler  
Rochester Institute of Technology

Ernest J. Dianastasis  
CAI

Amr ElSawy  
Noblis, Inc.

Roger A. Enrico  
DreamWorks Animation SKG Inc.

Alice P. Gast  
Lehigh University

E. Gordon Gee  
The Ohio State University

Robert B. Graybill  
Nimbus Services, Inc.

Nancye Green  
Waterworks

James W. Griffith  
The Timken Company

Amy Gutmann  
University of Pennsylvania

Brian L. Halla  
National Semiconductor Corporation

Peter T. Halpin  
World Resources Company

Jack Harding  
eSilicon Corporation

Patrick T. Harker  
University of Delaware

William C. Harris  
Science Foundation Arizona

Robert Hemenway  
The University of Kansas

Richard Herman  
University of Illinois at Urbana-Champaign

John C. Hitt  
University of Central Florida

Jerry MacArthur Hultin  
Polytechnic University of NYU

Mark V. Hurd  
Hewlett-Packard Company

Jeffrey R. Immelt  
General Electric Company

Ralph Izzo  
Public Service Enterprise Group Incorporated

Irwin M. Jacobs  
QUALCOMM, Inc.

John I. Jenkins  
University of Notre Dame

Paul G. Kimball  
Sagebrush Capital, LLC

Donald R. Knauss  
The Clorox Company

Carl F. Kohrt  
Battelle Memorial Institute

Robert W. Lane  
Deere & Company

Lester A. Lefton  
Kent State University

Michael A. McRobbie  
Indiana University

Alan G. Merten  
George Mason University

Richard K. Miller  
Franklin W. Olin College of Engineering

James B. Milliken  
University of Nebraska

C. Daniel Mote, Jr.  
University of Maryland

Eileen K. Murray  
Duff Capital Advisors

Mark A. Nordenberg  
University of Pittsburgh

Edward E. Nusbaum  
Grant Thornton LLP

Thomas F. O'Neill  
Sandler O'Neill + Partners, L.P.

James L. Oblinger  
North Carolina State University

**James W. Owens**  
Caterpillar Inc.

**Vikram S. Pandit**  
Citigroup Inc.

**Constantine Papadakis**  
Drexel University

**John D. Petersen**  
The University of Tennessee

**Peter G. Peterson**  
The Blackstone Group

**Dominic J. Pileggi**  
Thomas & Betts

**Judith A. Ramaley**  
Winona State University

**Robert L. Reynolds**  
Putnam Investments

**Peter J. Robertson**  
Chevron Corporation

**John A. Rollwagen**  
SiCortex

**John W. Rowe**  
Exelon Corporation

**Steven B. Sample**  
University of Southern California

**Leonard A. Schlesinger**  
Babson College

**Carl J. Schramm**  
Ewing Marion Kauffman Foundation

**Gary B. Schuster**  
Georgia Institute of Technology

**Bill Segura**  
Texas State Technical College System

**Ivan G. Seidenberg**  
Verizon Communications Inc.

**Joel Seligman**  
University of Rochester

**Scott D. Sheffield**  
Pioneer Natural Resources Company

**Robert N. Shelton**  
The University of Arizona

**Ruth J. Simmons**  
Brown University

**Lou Anna K. Simon**  
Michigan State University

**John B. Simpson**  
State University of New York at Buffalo

**Scott Sklar**  
The Stella Group, Ltd.

**David J. Skorton**  
Cornell University

**Frederick W. Smith**  
FedEx Corporation

**Christine J. Sobek**  
Waubonsee Community College

**Andrew A. Sorenson**  
University of South Carolina

**Mary S. Spangler**  
Houston Community College

**Graham B. Spanier**  
The Pennsylvania State University

**James D. Spaniolo**  
The University of Texas at Arlington

**Susan S. Stautberg**  
PartnerCom Corporation

**Charles W. Steger**  
Virginia Polytechnic Institute and State University

**Randall L. Stephenson**  
AT&T Inc.

**Robert J. Stevens**  
Lockheed Martin Corporation

**John A. Swainson**  
CA, Inc.

**John E. Treat**  
Alternative Hybrid Locomotive Technologies

**Steven L. VanAusdle**  
Walla Walla Community College

**Larry N. Vanderhoef**  
University of California, Davis

**George A. Vradenburg III**  
The Vradenburg Foundation

**Edie Weiner**  
Weiner, Edrich, Brown, Inc.

**Joseph L. Welch**  
ITC Holdings Corp.

**William C. Weldon**  
Johnson & Johnson

**William Weyand**  
MSC Software Corporation

**Timothy P. White**  
University of California, Riverside

**Sharon P. Whiteley**  
ThirdAge Inc.

**Jack M. Wilson**  
The University of Massachusetts

**James E. Wright**  
Dartmouth College

**Mark S. Wrighton**  
Washington University in St. Louis

**Henry T. Yang**  
University of California, Santa Barbara

**Paul A. Yarossi**  
HNTB Holdings Ltd.

**Nicholas S. Zeppos**  
Vanderbilt University

**Nancy L. Zimpher**  
University of Cincinnati

## National Affiliates and Council Staff

### NATIONAL AFFILIATES

American Association for the Advancement of Science  
 American Association of Community Colleges  
 American Council on Renewable Energy  
 AIGA  
 American Institute for Medical and Biological Engineering  
 American Mathematical Society  
 American Society for Engineering Education  
 ASME  
 American Society for Mechanical Engineers  
 Arizona Technology Council  
 Association of American Colleges and Universities  
 Association of American Universities  
 Association of University Related Research Parks  
 AVETeC, Inc.  
 BITS, Financial Services Roundtable  
 COMAP, Inc.  
 Council on Governmental Relations  
 Delaware Technology Park, Inc.  
 Detroit Renaissance, Inc.  
 Georgia Research Alliance, Inc.  
 IEEE-USA  
 Innovation Philadelphia  
 Innovation Works  
 International Economic Development Council  
 Iowa Business Council  
 JumpStart Inc  
 National Center for Manufacturing Sciences  
 National Center for Women & Information Technology  
 NEW CAROLINA  
 Northwest Food Processors Innovation Productivity Center  
 Northeast Ohio Technology Coalition  
 Nuclear Energy Institute

Oak Ridge Associated Universities  
 Rothman Institute for Entrepreneurial Studies  
 SMC3  
 Technology CEO Council  
 The Bi-National Sustainability Lab  
 The Conference Board, Inc.  
 United Negro College Fund  
 United States Council for International Business  
 University Economic Development Association

### COUNCIL STAFF

Deborah L. Wince-Smith  
 President  
 C. William Booher, Jr.  
 Chief Operating Officer and Treasurer  
 Cynthia McIntyre  
 Senior Vice President, Strategic Operations,  
 Planning and Development  
 Debra S. van Opstal  
 Senior Vice President, Thought Leadership  
 William C. Bates  
 Vice President, Government Affairs  
 Chad Evans  
 Vice President, Strategic Initiatives  
 Randall T. Kempner  
 Vice President, Regional Innovation  
 Mohamed N. Khan  
 Vice President for Information Services  
 Susan Rochford  
 Vice President, Energy & Sustainability Initiatives  
 Betsy Thurston  
 Vice President, Strategic Development  
 Patricia A. Hennig  
 Controller  
 Samuel Leiken  
 Senior Director, Policy Studies  
 David Padgham  
 Policy Director, High Performance Computing Initiative  
 Jennifer Carr

Communications Coordinator  
 Lee Dachi  
 Membership Manager  
 Marcy S. Jones  
 Executive Assistant to the President  
 Kara Jones  
 Research and Project Associate  
 Kara Guthrie  
 Research and Project Associate  
 James A. Knuckles  
 Research Associate  
 Maura Mondelli  
 Research Associate  
 Deborah Fletcher  
 Database Administrator

### COUNCIL FELLOWS

Erich Bloch  
 Distinguished Fellow  
 Daniel S. Goldin  
 Distinguished Fellow  
 Alexander A. Karsner  
 Distinguished Fellow  
 Alan P. Larson  
 Distinguished Fellow  
 Thomas J. Ridge  
 Distinguished Fellow  
 Edward J. Donnelly  
 Senior Fellow  
 Lisa Guillermin Gable  
 Senior Fellow

### COUNCIL ADVISORS

Jennifer Bond  
 Senior Advisor  
 Robert B. Graybill  
 Senior Advisor  
 Denise Swink  
 Senior Advisor

## About the Council on Competitiveness

### WHO WE ARE

The Council's mission is to set an action agenda to drive U.S. competitiveness, productivity and leadership in world markets to raise the standard of living of all Americans.

The Council on Competitiveness is the only group of corporate CEOs, university presidents and labor leaders committed to ensuring the future prosperity of all Americans and enhanced U.S. competitiveness in the global economy through the creation of high-value economic activity in the United States.

### Council on Competitiveness

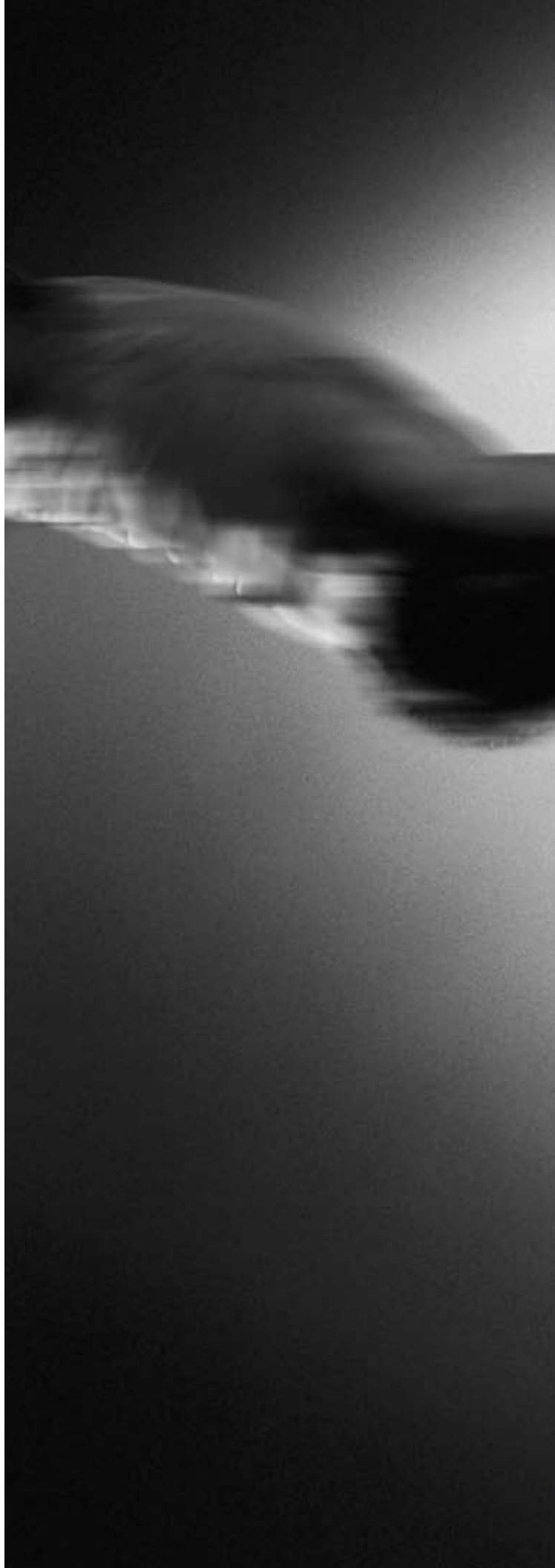
1500 K Street, NW  
Suite 850  
Washington, DC 20005  
T 202-682-4292  
Compete.org

### HOW WE OPERATE

The key to U.S. prosperity in a global economy is to develop the most innovative workforce, educational system and businesses that will maintain the United States' position as the global economic leader.

The Council achieves its mission by:

- Identifying and understanding emerging challenges to competitiveness
- Generating new policy ideas and concepts to shape the competitiveness debate
- Forging public and private partnerships to drive consensus
- Galvanizing stakeholders to translate policy into action and change



Council on Competitiveness  
1500 K Street NW, Suite 850, Washington, D.C. 20005 T 202 682 4292  
Compete.org



**Compete.**

Council on  
Competitiveness

