Why is Enterprise Risk Management Important for Preparedness?

by
Carol A. Fox, ARM
& Michael S. Epstein

Risk and Insurance Management Society, Inc.®

ERM
Center of Excellence

In his book, *The Upside*, Adrian J. Slywotzky presents a profound case for ERM and preparedness:

> Unmanaged risk is the greatest source of waste in your business and in our economy as a whole. Major projects fail; customer shifts make our offers irrelevant; billion-dollar brands erode, then collapse; entire industries stop making money; technology shifts or unique competitors kill dozens of companies in one stroke; companies stagnate needlessly. When these risk events happen, thousands of jobs get lost, brilliant organizations are disassembled, expertise gets lost, and assets are destroyed. Yet all of these risks can be understood, identified, anticipated, mitigated, or reversed, thereby averting hundreds of billions of dollars in unnecessary losses.[1]

Unmanaged risk … we all know that, in a world of constant change, things happen. Some things are within our control – most are not. However, the consequences of not being prepared for risk can have a damaging effect on our economy, our companies, our employees and the communities in which we operate.

Convergys' multiple southeast U.S. sites "weathered" the 2004 and 2005 hurricane seasons because of its preparedness efforts. Asked at a financial analysts' meeting about the effect the hurricanes had on Convergys' operations, Earl Shanks Chief Financial Officer replied, "Although we had damages, we went through the hurricane season without any material difficulty to the business. The preparation, the planning, and practice are keys to our effective business continuity effort." Using generator power, rerouting calls, and delivering needed supplies to our employees from unaffected sites al-

[1] The Upside: The 7 Strategies for Turning Big Threats into Growth Breakthroughs, by Adrian J. Slywotsky, Crown Business, an imprint of the Crown Publishing Group, 2007, p.231

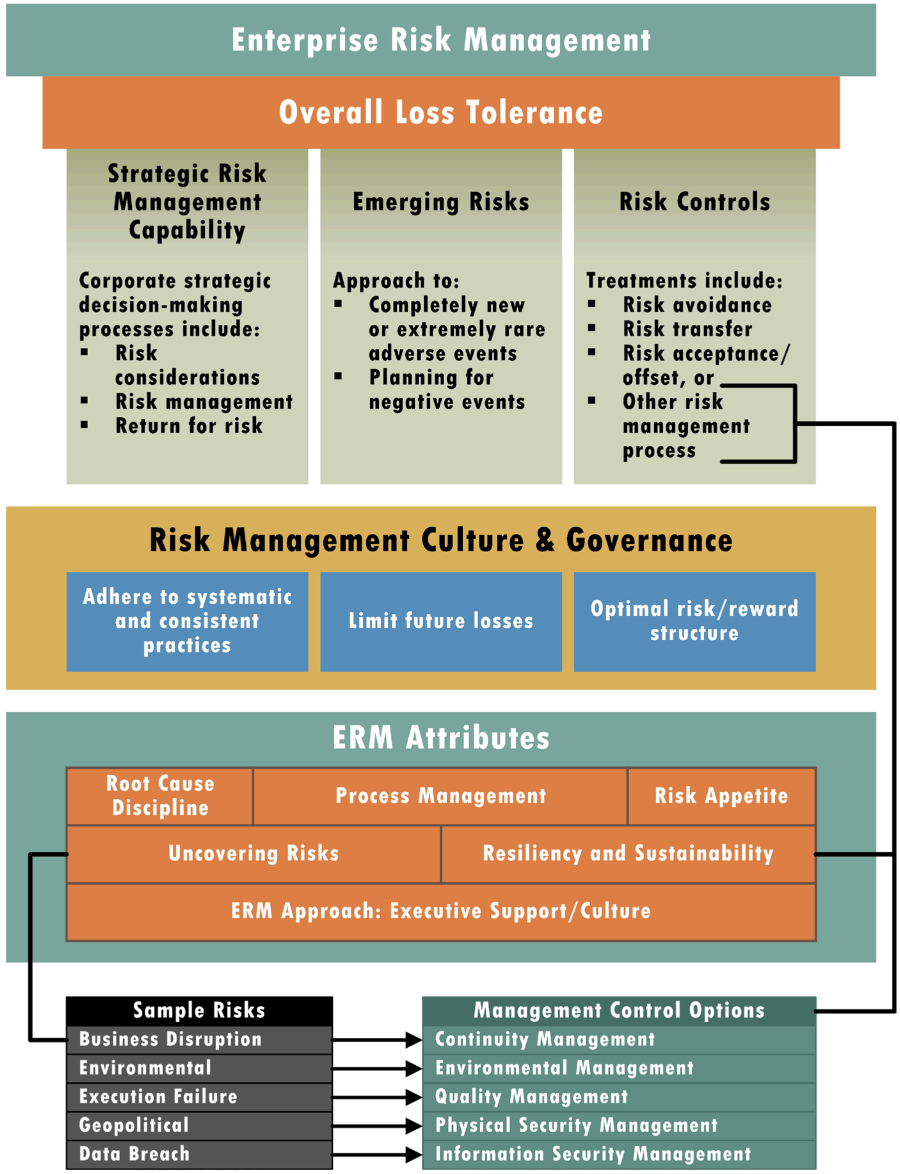
lowed us to continue business operations even in the devastated areas. One employee highlighted the personal economic impact of this particular risk while thanking our site leader for being prepared, "All I have left are the clothes on my back and the items in my purse. My house is gone, my car is gone, but I have a job and my neighbors don't."

The U.S. Congress recognizes the economic perils of not being prepared. In 2007, it directed the Department of Homeland Security to create a voluntary certification program to encourage private sector preparedness. In response, the Alfred P. Sloan Foundation commissioned a collaborative report, prepared by members of ASIS, DRII, NFPA and RIMS, to identify issues critical to the voluntary certification program's success and business viability. The resulting framework document[2] recommends that the certification program be **flexible**, contain appropriate **choices that meet respective business needs**, recognize the **common core elements** contained in various standards, and enable organizations to build on their **existing business continuity models**, within their **financial realities.**

The following diagram appeared in the framework document to illustrate how some companies have integrated preparedness into an overall ERM approach. The ERM attributes, or behaviors, included in the graphic are from the RIMS Risk Maturity Model©.[3]

[2] Framework for Voluntary Preparedness: A Briefing Regarding Private Sector Approaches to Title IX of H.R. 1 and Public Law 110-53 "Implementing Recommendations of the 9/11 Commission Act of 2007", January 18, 2008, is available without charge from the Alfred P. Sloan Foundation, ASIS, DRII, NFPA and RIMS websites.

[3] Risk and Insurance Society Risk Maturity Model©, 2006, www.RIMS.org



ERM views risk within an organization's unique **strategy**, **tolerance**, **culture** and **governance**. The programs generally provide for a consolidated view of emerging risks, including those that require planning for potential adverse events, by a cross-functional governing committee or council. This approach encourages flexibility. All ERM frameworks focus on the organization's overall business goals and objectives, the amount of risk the organization can tolerate, and what fits within its culture.

ERM uses **standardized**, **systematic** and **consistent practices**. Business Impact Analyses (BIAs) typically consider business impacts at a location or from a specific process based on a certain scenario or from a supply chain failure. ERM, on the other hand, considers business disruption risks comparatively measured against other risks an enterprise may face, using a standardized and consistent method. At an enterprise level, ERM programs generally apply qualitative and quantitative measurements through a risk assessment model. Rating and ranking all risks through consistently applied probability, immediacy and impact measures, while considering severity and reputation impacts, generates a priority scale across the organization. In the preparedness context, Convergys conducts risk assessments at an enterprise level, a site level, and at a program or project level.

Enterprise Assessment. Convergys is a global leader in relationship management providing solutions that drive more value from the relationships our clients have with their customers and employees. Working on behalf of our clients (including over half the Fortune 50), our 75,000 employees serve customers and client employees in 70 countries. Therefore, our enterprise assessment is global, and takes into account risks that could impede the achievement of our overall business objectives, both in the shorter term and in the longer term, using the practices noted above. The purpose of ERM is not the process itself, but as a method for management to focus on business solutions as it treats risk strategically and operationally. Business disruption is a risk that is important to our clients and to Convergys.

Site Assessment. Leaders at each site perform an assessment by analyzing and evaluating the potential risks. Using local infrastructure and neighbors as an example, we might ask, "What is the worst that can happen?" A single major highway running near the site may represent a risk to the facility should there be a chemical spill. That spill may not affect operations at the site directly, but it may prevent staff from accessing the facility for a significant time. Neighbors represent potential hazards either as a direct result of their respective businesses or because of threats to the businesses. Those threats could affect the key resources supporting our business. A neighboring company may work with hazardous materials, or it may perform controversial activities and result in a demonstration that could disrupt our resources. Assessing the risk impact from a worst-case perspective, and evaluating the controls that are already in place, directs our planning efforts.

Program or Project Assessment. The assessment of a program's or a project's capabilities, resources and limitations are core to the development of a viable recovery strategy. This includes consideration of location, technical infrastructure, physical and staffing resources required to support operations. Decisions made in the contracting process drive the recovery strategy. Who will perform the work? What vendors will be supporting the same or related business for the client? What is the geographic distribution of the work? What skills are required, and where are they available? What are the needed recovery time objectives? Each of these aspects influences our planning for a potential disruption.

ERM enables an organization to **prioritize and allocate resources** against those risks that underpin the continued sustainability of the organization. In other words, an organization's ability to maintain something of value (such as the delivery of services or products to customers) relies on its ability to understand and plan for those risks that may impede the achievement of its business objectives / goals or risks that could significantly impair its capital.

ERM uncovers risks in order to **build organizational resiliency and sustainability**. Organizational resiliency, or an enterprise's ability to recover quickly from setbacks, is particularly important when a risk is unavoidable or non-transferrable. Do we understand the root causes of the risk event? Is the risk acceptable within our risk tolerance? Do we have the appetite to take on more risk? If not, how can we prevent, mitigate or exploit the risk event (or its likely consequences)? What controls are in place to manage the risk?

ERM ties uncovered risks to controls found in established management systems. Is business disruption risk being controlled by the organization's continuity management program? Is environmental risk being controlled by its environmental management system? Is regulatory risk being controlled by a compliance program? Does every uncovered risk have an established management system or program? If not, who within the organization owns the risk? Does current strategic or operational planning appropriately consider the risk? If not, what else is required?

ERM, through partnership with Internal Audit, monitors the organization's confidence in the established control systems for managing the uncovered risks. In conjunction with other risk stakeholders, the ERM framework provides for evaluation of these management control programs / processes and systems. On a High, Medium or Low scale, how confident are we that the controls have been deployed, maintained, and monitored? Are the controls effective? When operations change, do controls change too?

ERM encourages cross-functional discussion of potential unintended consequences. By establishing risk reporting as part of management's normal business reviews – at whatever frequency makes sense for the organization – the decision-makers have a broader perspective of the risk interdependencies. These interdependencies relate not only to the risks themselves, but include the respective risk treatments undertaken for each risk.

At Convergys, the Business Continuity Planning Group exists within the greater ERM framework and reports directly to risk management. The benefits of this arrangement are multiple. Key risks gathered as part of the ERM effort serve as direction setters for business continuity. The business continuity planning processes may uncover issues the ERM program will be required to address. The priorities and risks identified by ERM enlighten the continuity planning process, resulting in more focused and effective planning. Senior leadership participation from a global perspective under ERM, in conjunction with a root cause discipline and controls assessment, is much more effective in identifying and assessing key risks than typically is realized in a traditional BIA. At the same time, the comprehensive view provided by the ERM framework results in a higher level of visibility for continuity related issues. As decision-makers take a concentrated look at their risks, they address current and potential controls. As a result, Business Continuity Planners become critical players in controlling a range of disruptive risks.

Whether your organization decides to seek the voluntary preparedness certification or not, the questions to ask are, "How prepared are we to manage the risk of business disruption? How well do we understand, identify, anticipate, mitigate - or can we reverse - that risk, thereby averting … unnecessary losses?" Your organization's sustainability and resiliency – and the economic well-being of your employees (nay, the very nation) – are relying on your answers. ■

About the Authors

Carol A. Fox, ARM is an ERM expert and has authored and contributed numerous articles and whitepapers on risk management topics for a wide range of publications. She contributed to the development of the RIMS Risk Maturity Model, and is a regular presenter at risk management forums.

Carol has served on the Board of Directors of the Risk and Insurance Management Society, Inc. (RIMS), a not-for-profit association dedicated to advancing the practice of risk management, as well as on the Board of Directors of the nonprofit Spencer Educational Foundation.

In 2009, Carol was presented with RIMS' most prestigious recognition, the Harry & Dorothy Goodell Award, for her outstanding achievements in advancing the risk management discipline.

Michael S. Epstein is a senior manager of business continuity planning for Convergys Corporation, where he is responsible for coordinating the development, testing and maintenance of business continuity plans across Convergys Corporate & Divisional businesses as well as supporting acute incident response across the enterprise. Key incident repsonses he had been involved in include Typhoon Onday (September 2009, Philippines), the H1N1 pandemis (2009, global), and Hurricane Ike (September 2008, Gulf Coast and Midwest U.S.).

About RIMS

The Risk and Insurance Management Society, Inc. (RIMS) is a not-for-profit organization dedicated to the advancing the practice of risk management. Founded in 1950, RIMS represents more than 3,500 industrial, service, non-profit, charitable and governmental entities. The Society serves more than 10,000 risk management professionals around the world.

This white paper is published by RIMS with permission of the author and contributions from the RIMS ERM Committee.

For more articles, white papers and resources on enterprise risk management, visit the RIMS ERM Center of Excellence at www.RIMS.org.