



*THE FUTURE OF
ENTERPRISE RISK MANAGEMENT*

*ENTERPRISE RISK MANAGEMENT ROUNDTABLE SUMMARY
DECEMBER 3, 2009*

A Terry College of Business and Sunera Partnership Event

Overview

The Enterprise Risk Management Roundtable was created by Sunera (<http://www.sunera.com>) in partnership with The University of Georgia's Terry College of Business. The UGA Risk Management and Insurance program (<http://www.terry.uga.edu/insurance>), currently ranked # 2 in the country by U.S. News and World Report is led by our moderator, Dr. Rob Hoyt.

The goal of the Roundtable is to promote thought leadership around enterprise risk management (ERM) while facilitating networking opportunities for attendees. By joining both the academic and business communities through this endeavor, our goal is to promote thought leadership of enterprise risk management as well as to discuss effective strategies for implementing and nurturing the risk management practices within today's businesses. This invitation-only program is designed for peer-to-peer discussion while promoting meaningful relationships within the Atlanta market. The Roundtable topics are selected based on relevance to a wide range of industries and attendee job responsibilities.

Our first Roundtable was held on December 3, 2009 at the University of Georgia's Executive Education Center, located in the Buckhead area of Atlanta, Georgia. The format represented an academic approach to the history of enterprise risk management and how industry leaders have interpreted and are implementing ERM.

Dr. Rob Hoyt provided the academic perspective, and our industry keynote speaker was Rick Machold, Head of Enterprise Risk at Invesco who was followed by a panel discussion featuring three prominent ERM professionals from the Atlanta market. Our panel included Keith Cureton, United Parcel Service (UPS); Greg King, Rock-Tenn, and Phil Maxwell, Coca-Cola Enterprises (CCE); who all shared a brief overview of their interpretation and implementation of ERM initiatives at their respective companies. After concluding opening remarks by the panelists, a 30 minute question and answer period followed for all roundtable participants to engage in dialogue with the presenters.

Academic Perspective



Dr. Rob Hoyt, Moore Chair and Professor of Risk Management, Terry College of Business, University of Georgia

As indicated, Dr. Hoyt brought the “academic perspective” to the ERM Roundtable – he suggested that some might argue that academic is synonymous with irrelevant, theoretical and impractical. However, his goal is to provide a bit of context to today’s discussion by reflecting briefly on the history of ERM and the current state.

Historically, many new developments in business have followed theoretical development in the academic sector. Take for example the pricing of derivative securities. In contrast, for ERM the pattern of development between theory and practice has been much more contemporaneous. It might even be argued that for ERM, it’s been a case of the science catching up with the practice.

The History

Way back – until external capital markets developed and we had widespread separation of ownership and control, integration of risk management was not an issue – to the extent risk management was done. Note that in a 1999 study that Rob performed, he found that corporate comfort with the degree of risk management integration was higher for smaller and larger firms (they called it the ‘risk management smile’). The separation of ownership and control in modern corporations contributes to the importance of corporate governance.

So it isn’t surprising that early and continuing developments toward ERM have often had a governance theme. To give some context, Rob provided a few important events along the ERM development timeline:

- | | |
|--------|---|
| 1970’s | Some early ideas of holistic risk management date back to the 1970s in Sweden by the risk manager of a state-owned business conglomerate, Statsforetag |
| 1992 | The Cadbury report in the UK and the ensuing Cadbury Code put the ultimate burden of risk management on the corporate directors

Committee of Sponsoring Organizations of the Treadway Commission's (COSO) internal control framework was published |
| 1993 | The origins of the Chief Risk Officer (CRO) title appears to go back to 1993 at GE Capital – the position was held by James Lam, still active as an ERM proponent and consultant |

Enterprise Risk Management Roundtable: Executive Summary

- 2002 The Sarbanes-Oxley Act (SOX) - Section 404 was legislated and it can be argued that it pushed the risk management process along (although with an emphasis on controls and compliance, and not as much on strategy).
- 2003 In insurance, the Casualty Actuarial Society published an overview on ERM.
- 2004 In banking, BASEL I, addresses quantifiable and less quantifiable risks
- COSO Enterprise Risk Management- Integrated Framework was published and has been important in framing ERM development in the U.S.
- COSO's definition of ERM : "a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

On the academic side, specific college courses and course content on ERM began emerging as far back as the late 1990s and has continued to expand. Academic research on ERM has been evolving in disciplines including accounting, finance, insurance and management. Curriculum/research which has added to the risk management body of knowledge includes a 1999 paper on integrated risk management, 2001 survey of CRO's, 2003 determinants of adoption, and a study in 2009 on the value of ERM.

ERM Internationally – Dr. Hoyt suggested that some would argue that ERM development moved ahead earlier and faster outside the U.S., the following are a few additional key dates and facts in ERM development internationally:

- 1998 In Germany – KonTraG is the law for Control and Transparency and has led to big changes in corporate governance and has improved internal control systems for German firms
- 2005 In Canada, Bill 198, aka C-SOX, is similar to the US SOX standards and applies to all firms listed on the Toronto Stock Exchange
- 2009 In Australia and New Zealand, arguably the first effort at developing an international standard for ERM, AS/NZS 4360, the emerging ISO 31000 standard is intended to be a family of standards relating to risk management codified by the International Organization for Standardization.

The Current State

Dr. Hoyt posed the question of “What have we learned from some of the many surveys directed at assessing the current state of ERM?”, and provided some key items from two recent surveys:

In a 2008 survey by Treasury & Risk Management:

- Strategic risks still viewed as the most difficult to assess and manage
- Biggest challenges to fully implementing ERM
 - conflicting priorities
 - difficulty quantifying risks
 - difficulty embedding risk management into culture

In a 2009 survey focused on financial institutions by Deloitte:

- 77% stated that the board has ultimate responsibility for risk
- 73% had a CRO
- 85% of firms with ERM in place said the benefits outweighed the costs
- Increase in the level at which reporting takes place from 2006-2009
 - 37% to 52% reporting directly to the board
 - 42% to 53% reporting directly to the CEO
- Highest value of ERM in the financial sector
 - improved understanding of risk
 - improved perception by the regulator (in these highly regulated industries)
 - ability to escalate critical issues to senior management

Value of ERM – in a current UGA study of publicly-traded insurers, UGA found a 17% market value premium for ERM adopters.

S&P’s 2009 announcement regarding the inclusion of ERM assessments in its ratings and the proposed SEC guidelines on disclosures about the board’s involvement in the risk management process is also likely to provide additional impetus for firm’s to focus more attention on ERM.

In Summary

Rob concluded his remarks by stating:

- ERM is here to stay
- One-size doesn’t fit all
- The key question is: How does your organization appropriately integrate risk management into your processes in a manner that achieves maximum benefit? In the

remarks and discussion that will follow today we hope to provide some valuable insights into the answer to this question.

Industry Perspective



Rick Machold, Head of Enterprise Risk, Invesco Ltd.

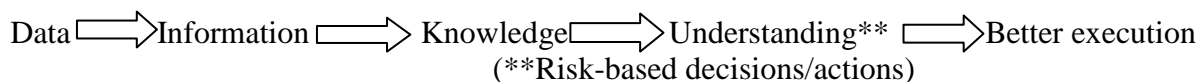
Rick's ERM perspective is one of process and organization whereby he thinks in terms of organization and process constructs to determine the means of successfully guiding the ERM program within Invesco. In these current times, there is a lot going on, things seem to be blowing up all around us (think of our economy, corporate scandals, ponzi

schemes in the news, etc) and ERM is ubiquitous (defined as being or seeming to be everywhere at the same time; omnipresent) with a lot of focus and fingers pointing towards "risk management failures." Not all recent failures have been risk management. Sometimes, people or business leaders take well informed risks in guiding their business, and it simply does not work out. How we respond to risk is critical, and making sure ERM is relevant while providing practical, demonstrable value to the organization will determine the success or failure of an ERM program. A few of the value killers are:

- Focus is on consequences and expedient, symptomatic solutions
- Poor ability to manage complex, dynamic risks and interrelationships
- "Delusional optimism," where managers are lulled into a false view of outcomes, choosing to focus on the best case scenario rather than what's likely or realistic

Ideally, ERM should be "a rational response to an increasingly risky world." One of the keys going forward is developing our ability to see the future clearly, factually, and make well-reasoned predictions as to what is likely to occur.

A common result of a post crash or catastrophic event is lots of activity to fix the problem and at times, an over-reaction of well-intentioned legislation which drives an over-reaction by others. One fear that surfaces is that ERM will take on a compliance focus and people end up getting lost in all the detail and activity (remember the early years of SOX). Machold believes that one way to depict a value-add ERM process is as follows:

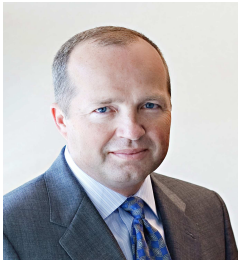


Real value is found not in data, information, or knowledge but the understanding that results from processing data to create information which leads to increased knowledge and ultimately to understanding. An unfortunate outcome of some ERM programs is that the "rubber never meets the road," (i.e. the good work done in processing data never actually gets used in risk-based decision making). Value is also found in the dialogue and whether the business is

actively engaged in discussing risks, how to manage risks, or whether to control, avoid, insure, or accept risks. This dialogue and discussion will lead the ongoing evolution of a successful ERM program. Another key ingredient is finding people within your organization that possess the right combination of experience and understanding resulting in them providing their instinctive judgment as to which risks the business needs to manage best.

In his bestselling book, *Blink*, Malcolm Gladwell discusses the concept of “thin-slicing” in great detail, and proposes that instinctive judgment can at times, be a better way to solve very complex problems. The idea is that a person’s instinctive subconscious, if given the right amount of experience, context, and truth, can deliver the best solution to complex problems instinctively and without conscious thought. Gladwell summarizes that the key to good decision making is to understand that one of the great challenges of our time is how to combine the best of conscious deliberation and instinctive judgment.

Machold suggests that certain key leaders within your organization could possess the ability to size up a situation purely on instinct and make the right decision providing a critical input into the organization’s ERM process. He also recommends relentlessly evaluating your ERM program, questioning the value your program is delivering, and challenging what you are doing today. Determine your proof points of an effective ERM program, verifiable outcomes of good risk management, and use hindsight to look for ways in which your ERM practices have truly made a difference. One of the key challenges going forward will be continue to be articulating the value of ERM within your organization.

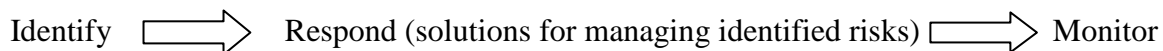


Keith A. Cureton, Corporate Group Manager for Enterprise Risk Management, UPS

Keith began his discussion by pointing out that culture plays a huge role at UPS in terms of how a successful ERM program needs to function and that relationships within the organization are key in understanding the organization’s business initiatives. The organizational structure for ERM

within UPS traditionally focused on where there was a passion for risk management, which originally was within the treasury function. Today, ERM, Internal Audit, and Compliance & Ethics functions all report up to the audit committee and are all connected to the management committee, corporate strategy group, and enterprise risk council. This evolving structure is a sign that risk management today is a focus of the entire organization and no longer only a treasury concern.

Cureton explained that within UPS the ERM function focuses on managing the process and that various business managers throughout the organization are responsible for ensuring that agreed upon risks are mitigated to an acceptable level. The overall process can be depicted by the following diagram:



The enterprise risk council focuses on an ongoing review of identified risks and the Corporate Group Manager for ERM monitors the responses to ensure that the solutions for managing risks are implemented by the organization in a timely manner.

UPS uses various tools to manage the risk management process including a risk & control framework which is used to manage each identified risk and group the risks into an ERM model which leverages the COSO ERM framework. These tools help to facilitate strategic, operations/infrastructure, reporting, and compliance throughout the organization. The framework articulates the risks, identifies how the company manages the risks, and references who owns the risk. In addition, UPS utilizes a risk heat map which references the status of where the organization is at with managing risks and the mitigation strategy outlined for each risk. Each risk is evaluated to ensure the risk links to the corporate strategy. When identifying risk, UPS always states the risk in terms of “There is a risk that” The business then completes the sentence in identifying relevant risks to the organization. Keith wrapped up his presentation by stating “he is just a process guy who helps provide a way to manage risk throughout the organization”.



Gregory King, Vice President of Risk Management, Rock-Tenn

Greg stated that an overriding goal for the ERM program within Rock-Tenn is to assist the organization to avoid the big mistake and to systemically identify, understand, and manage risk to optimize business results. Using these key guiding principles, RockTenn’s approach to manage risk begins with identifying strategic risks which could impact the

core business. Then, they focus on specific business risk which threatens the ability of the division management to execute in accordance with the strategic plan of the company. Other risk areas addressed include outside risks such as commodity risk, the risk that prices for commodities fluctuate, which could have an adverse effect on the company.

King mentioned that the process of monitoring and anticipating changes to the economic, political, and regulatory environment is important in making sure that all the relevant risks are being identified and managed in a timely manner. Also, monitoring and managing business risks and possible business disruptions are central to helping the organization optimize business results. In total, the company is currently managing over a hundred key risks which involve eight main business processes throughout the organization. The risk assessment process supports the annual audit planning process. Audit priorities are then classified by the business into four main areas: first tier audit focus, second tier audit focus, management discretion, and limited audit focus.



Phil Maxwell, Director of Enterprise Risk, Coca-Cola Enterprises

Phil opened his remarks by supporting the previous panelist's opinion that your company culture is an integral component in evolving your risk management process. Your culture needs to imbed the risk management responsibility within the operations of the company. A risk management capability curve shows the risk

management capability on the horizontal axis and stakeholder value on the vertical axis, as you progress with your risk management process, you should be moving down the horizontal axis and up the vertical axis. Keeping track of the progress will allow you to measure how successful your risk management process is and will provide you the feedback to continue to reinvent the process to keep moving forward. Maxwell mentioned that CCE is an operational company which was built over the years through many acquisitions. Continually evaluating how to make the risk management process successful and doing what is best for the company are cornerstones of his program.

Maxwell's approach is straightforward and involves leveraging the existing business processes within the company while ensuring that risk management is embedded within these processes. Promoting a risk management process and not an acronym (i.e. ERM) while aligning your priorities to the key organization's objectives and strategies, will keep your process moving forward and aligned to the company strategy. The project selection process begins by looking at the long term goals of the company and asking the question, does this project make sense and is it aligned to these organizational goals, are how Coca-Cola Enterprises prioritizes ongoing risk management and business initiatives.

Phil wrapped up his comments by suggesting that he has found best practice to include ensuring your program has the appropriate executive sponsorship, yields tangible results, and adds value to the organization. Coordination is the key, not inventing new processes. Managing expectations and practicing patience with persistence will help you in leading your organization down the risk management curve.