2009

Real Insights on ERM Implementations

2008–2009 ERM Roundtable Summaries

As expectations for stronger risk oversight emerge from the recent economic crisis, boards and senior executives are seeking ways to strengthen their approaches to enterprise-wide risk management. This document contains summaries from five ERM Roundtables hosted by the ERM Initiative at North Carolina State University in fall 2008 and spring 2009. Real-world ERM implementation examples from H.J. Heinz Company, the State of Washington, and KBR Inc. are provided in addition to emerging ERM insights from Standard & Poor's and the New York Stock Exchange.

ERM Initiative at North Carolina State University (www.erm.ncsu.edu)

Overview

Enterprise risk management—an integrated approach to effectively identifying, assessing, measuring, and managing the complex and interrelated risks across an enterprise—has emerged as a critical element of many organization's overall strategy for maximizing the creation and preservation of value for its stakeholders. North Carolina State University's ERM Initiative is uniquely positioned among institutions of higher education and internationally recognized for its leadership in the proactive management of entity-wide risks in an increasingly competitive global business environment.

The ERM Initiative regularly hosts ERM Roundtables designed to bring executives with risk management responsibilities together to dialogue about emerging issues affecting ERM practices. As of April 2009, the ERM Initiative has hosted thirty-seven of these events, featuring business professionals, including chief risk officers, members of boards of directors, and other risk management experts.

The ERM Initiative at NC State is providing this synopsis of our 2008—2009 ERM Roundtable presentations to share information on effective ERM practices gleaned from these events. These Roundtables provided rich real-world insights from ERM leaders at H.J. Heinz Inc., the State of Washington, and KBR, Inc. who shared in-depth illustrations of how they are tactically implementing critical components of effective enterprise risk oversight. In addition, our February 2009 ERM Roundtable hosted in Charlotte, NC featured Steve Dreyer who provided an overview of Standard & Poor's current evaluations of enterprise risk management practices performed in conjunction with their credit risk assessment processes. Following that, our March 2009 ERM Roundtable featured Glenn Tyranski, Senior Vice President of Financial Compliance at the New York Stock Exchange (NYSE), who provided perspectives from the NYSE about governance and risk management.

This collection of ERM Roundtable summaries contains practical insights that may be helpful to senior executives and their boards of directors in strengthening their enterprise-wide risk oversight. Summaries of all prior ERM Roundtables can be obtained by visiting the "Resources" section of the ERM Initiative's website (www.erm.ncsu.edu).

Our goal is to provide thought-leadership to assist organizations seeking to more fully develop their enterprise risk oversight by strengthening its integration with strategy planning and corporate governance. Additional resources related to enterprise risk management are also available at the ERM Initiative's website. Under the "Resources" link, synopses of over 150 articles and whitepapers are available. The ERM Initiative publishes an electronic "ERM in the News" newsletter—interested recipients should register for these twice-monthly free newsletters by following the link on our website. The ERM Initiative also provides executive education for boards and senior executives on effective ERM practices.

Mark S. Beasley

Deloitte Professor of Enterprise Risk Management

Bonnie V. Hancock

Executive Director, ERM Initiative

Bruce C. Branson

Associate Director, ERM Initiative

Linkage of Reputation and Risk Management

Jim Traut, H. J. Heinz, Inc.
October 2008 ERM Roundtable

The H.J. Heinz approach to ERM is positioned to be value-adding by focusing their efforts on supporting long-term sustainability of the organization. This is evident in the company's published mission statement that focuses on results that balance both short-term and long-term value-drivers. The ERM program at Heinz is formally known as "Enterprise Reputation and Risk Management (or ER^{2}M)." Heinz's ER^{2}M helps enable the company meet two primary reputation-related goals: to further support their objective of doing the common thing uncommonly well and to position Heinz as the most trusted packaged food company.

Strategic Focus of Risk Oversight

Risk at Heinz is defined as "anything that can prevent the company from achieving its objectives." In formalizing an ERM process, Heinz identified risks and events the company experienced or may experience and divided those risks into two main areas: operational risk areas and non-operational risk areas. Operational risks include product quality, environmental & sustainability, employee health & safety, facility and product security, business continuity and asset conservation. Non-operational risk areas include strategic and market, corporate governance and ethics, financial, legal, information services and human resources.

ERM is designed to enable leaders across the organization to be risk aware, not risk averse

Heinz's approach to ERM is designed to enable leaders across the organization to be *risk aware*, not *risk averse*, with a primary focus on protecting and thereby maximizing enterprise value and brand equity. ERM is viewed as a way to achieve competitive advantage by engaging in risk oversight activities that preserve or enhance the company's reputation. Heinz's ERM program is not positioned as a compliance reaction to regulations.

There have been five main ERM priorities Heinz has focused on to date:

- Establishment of the ER^{2}M structure
- Development of the Heinz ER^{2}M methodology
- Conducting top-down risk assessments
- Mitigation of top risks
- Global standardization and measurement of operational risk areas

Establishment of the ER^{2}M Structure

In response to the audit committee's desire for improved risk oversight, Heinz's management team established an Office of Risk Management in May 2006 that reports directly to a Senior Vice-President in the company and interacts with internal groups including the audit committee, disclosure committee, and corporate internal audit. These interactions help ensure global risk ownership, ongoing risk oversight, input into annual report risk factors, identification and prioritization of risks, linkage of key risks and resources, alignment of risk appetite with controls, input into the annual audit plan, and continuous improvement. The company also has a Risk Council comprised of senior leaders in each functional risk area. Within Heinz, ERM is positioned to provide a unified, global, cross-functional approach to identify, prioritize, measure, and manage key business risks. Key components of this approach are that ERM will drive global facilitation, best practices, compliance, and continuous improvement; accountability for and ownership of risks and mitigation plans at the appropriate management level; and a common integrated global process to manage risks and mitigation activities across all risk areas.

Development of the Heinz ER²M Methodology

The risk management model at Heinz was leveraged off an existing health and safety prevention pyramid model widely embraced across the company that combines preventative processes; emergency planning and response; crisis planning, communication, and response; and contingency planning and business continuity management. This model helps focus risk management activities on what is important for Heinz— preserving and enhancing the company's reputation in the packaged food industry. Reputation risk is always a consideration as it encompasses all of the other risk areas Heinz considers.

Reputation risk is always a consideration as it encompasses all of the other risk areas Heinz considers

There are six steps in Heinz's **ER²M** methodology for global and business unit level risk: maintain awareness of existence of events that could prevent the company from achieving its objectives, develop and analyze measures of the likelihood and impact of events in a disciplined way, prioritize events with cross-functional and enterprise-wide rankings, take action to mitigate risks by preventing or reducing probability and impact of an event or by purchasing insurance to reduce financial impact, integrate mitigation processes into ways Heinz conducts its core business, and seek to continuously perform the other five steps. The goal of ER²M at Heinz is to develop a risk aware versus a risk avoidance culture; therefore some risks will remain after all of the steps are completed. As part of the process, management continually evaluates remaining residual risk.

Conducting Top-Down Risk Assessments

Heinz has gone through two top-down global risk assessments since May 2006 and plans to continue this process annually. This process refines the risk inventory for each functional area from a brainstorming list to the top three to five critical risks based on analysis of risk data, control activities, risk ranking scores, and recommendations for filling gaps. An important component of this assessment is that each functional risk is reviewed from a strategic perspective with a three-year time frame, emphasizing Heinz's focus on the long-term horizon. Findings are validated with the executive risk owner in each functional area and then the validated list is reviewed with the Risk Council. These top risks and mitigation efforts are then reviewed with senior management. The result of this process is that Heinz has a list of the top risks of the company for that year, along with the actions being taken to address those risks and the global owners and process owners of each risk. Top risks facing the company along with action plans are presented to the audit committee.

Lessons Learned

From Heinz's entry into ERM, Traut shared these lessons learned:

- Board of Director and executive level support is critical for success
- Establish risk management ownership by functional area
- Encourage open discussions of "what keeps people up at night"
- Convert initial lists of "worries" to actionable risks
- Respect and protect anonymity of risk assessment participants
- Communicate regularly, thoroughly, and top to bottom to ensure support for ERM efforts
- Measure risk mitigation efforts via scorecards
- Customize ERM to your culture and ways of working
- Develop mindset that ERM is a cultural journey rather than a project destination
- Position ERM to drive synergies as the whole will be greater than the sum of the parts

Traut concluded by reminding the audience that ERM's goal is to ensure that Heinz continues its 140-year history of "doing the common thing uncommonly well" so that the company's sustainability is ensured throughout the next century.

Relevance of ERM for Government

Drew Zavatsky, State of Washington
November 2008 ERM Roundtable

In Washington State, ERM implementation has been a stated organizational best practice of the governor since 2006. ERM implementation efforts for the largest state agencies are reported during Government Management, Accountability, and Performance (GMAP) forums, in which the governor is updated about progress on key agency activities. Since beginning the state's ERM implementation efforts, the state has been able to decrease its self-insurance for its liability fund by $40 million, representative of a much larger decrease in expected liabilities, likely attributable at least in part to ERM practices. Future ERM efforts in Washington include sharing ERM implementation best practices with all state agencies, increasing participation opportunities to more agencies, and creating a state enterprise risk register.

Developing ERM in State Agencies

The goal for the Loss Prevention Group, a group in the Washington State Office of Financial Management's Risk Management Division, is to foster ERM implementation in all 165 state agencies. The Group developed ERM practices based on activities already used by state agencies. In implementing ERM, the Loss Prevention Group emphasizes flexibility, ease of training and use, and low costs to demonstrate how ERM can add value to an agency. ERM training sessions for agencies range from thirty-minute sessions for executives to two-day sessions where two day-long sessions are scheduled a few weeks apart to allow agency personnel to start implementing their ideas and come back to the second session and refine their ideas. Training sessions emphasize that ERM techniques are straightforward and apply just as easily to situations in everyday life. During a session, agency personnel refine their goals, identify risks to achieving those goals, and then work together to identify a short list of priority risks that should be addressed.

Reporting on ERM Implementation Efforts

Once a year, during the governor's GMAP forums, ERM maturity model scores of the largest state agencies are reported. Twice a year, these agencies are responsible for reporting on ERM, with annual updates on ERM implementation successes and best practices. The maturity model helps to assess ERM progress and it measures ERM in five areas: fundamentals of risk management, executive leadership, ERM integration into agency culture, application of ERM principles, and how embedded ERM is in agency strategic business operations. Maturity model scores ranged from 2—6 and, in 2006, only four of the agencies reporting on ERM were at a maturity level 5, while in 2008, all thirty-two of the agencies reporting were at maturity level 5 or 6. One advantage of the maturity model approach is that it provides an identical tool for use in assessment across the state so it is easier to see which programs are working well and which could use improvement. In addition to maturity mapping, these thirty-two largest state agencies are on a three-year roadmap for implementing essential ERM functions.

ERM …starts by looking at all the important goals in the agency and all of the positive and negative risks that can prevent reaching those goals

ERM Training Session Messages and Benefits

There are several core messages the Loss Prevention Group seeks to convey in ERM training sessions for agency personnel. One message is that while there is no one correct risk appetite, it is important to know what the agency's risk appetite is since different people could make different decisions based on the same set of facts. Sessions also address the idea that risk is usually thought of in a negative connotation. Participants are reminded that there is no opportunity without risk and in every risk there is an opportunity. Another key message is that ERM does not involve implementation of an entirely new set of principles. Rather, ERM is merely an enhancement of traditional risk management approaches that starts by looking at all the important goals in the agency and all of the positive and negative risks that can prevent successful attainment of those goals.

There are also several key benefits ERM implementation can provide to state agencies. ERM helps to prioritize which risks to avoid, accept, reduce, or share. Also, because some risks cannot be controlled, ERM can help by having a plan for those risks and in determining the amount of resources to devote to those risks. ERM is a repeatable and scalable process that is time-specific and success-oriented that can help in refining goals, improving communication, and allocating resources where they are most needed.

Seven-Step ERM Method

Each agency is trained to use a Seven-Step ERM Method to conduct risk assessments that includes the following actions:

1. **Clearly state the goal**. The goal should be stated in the positive, be specific and precise, and have a finite timeframe.

2. **Identify risks to achievement of these goals.** List everything that could keep you from meeting the goal, whether positive, negative, large, or small that could prevent reaching the goal in the defined timeframe. The list can be developed by a risk manager, others in the agency, and even include subject matter experts external to the agency.

3. **Evaluate each risk**. Choose a likelihood rating from 1–5 and an impact rating from 1–5. The ratings may vary for different agencies that have different impacts of concern. Voting on likelihood and impact scores should be done anonymously to avoid bias.

4. **Prioritize the risks**. By multiplying the likelihood and impact scores, a risk map can be created. Priority risks are often the most severe risks that are both likely to happen and will have a large effect, but that is not always the case. Sometimes the frequent but minor risk that in the aggregate could have a very large impact or the rare but significant risk may also be important to address. The map also serves as a document showing stakeholders the reasons for the decisions made.

5. **Respond to priority risks**. Responses may involve avoiding, accepting and monitoring, transferring, reducing the likelihood, or reducing the impact of the risks. In accepting and monitoring a risk, put a system in place so that if the risk exceeds a certain level it will be addressed. The treatment that is chosen should fit the risk appetite of the agency, reflect the amount of control over that risk, be measurable, and have a definite timeframe. This approach allows resources to be directed to the most important risks.

6. **Compile a Risk Register.** The Risk Register is a list of priority risks and an overview of how each will be handled. The goal should be listed, along with the priority risks to achieving that goal including descriptions of the risk, risk scores, level of control over the risk, treatment chosen, description of treatment plan, measures that will show success, target dates, and the person responsible or risk owner. This treatment plan should be monitored and refined periodically as ERM is an iterative process, not a one-time effort.

7. **Communicate results**. This can be accomplished by gathering and sharing best practices, reviewing any gaps, and reassessing and refining practices.

Several of the ERM tools used by the state of Washington are available on the state's Office of Financial Management's website: http://www.ofm.wa.gov/rmd/default.asp

S&P Evaluations of ERM as Part of the Credit Ratings Process

Steve Dreyer, Standard & Poor's
February 2009 ERM Roundtable

Standard & Poor's announced in 2008 plans to include evaluations of how effectively non-financial companies manage enterprise-wide risks as part of S&P's credit ratings process. Steve Dreyer, Managing Director of Utilities and Infrastructure Ratings at Standard & Poor's, provided an overview at the February 2009 ERM Roundtable in Charlotte about S&P's process for evaluating ERM practices as a part of their overall analysis.

Motivation for Considering ERM

S&P's decision to look carefully at how companies manage enterprise-wide risks is directly linked to the credit rating agency's desire to more accurately assess the predictability of a non-financial company's likelihood of repaying its financial obligations. In S&P's view, the economic events of the past year underscore the need for better risk oversight for entities of all types. S&P is interested in obtaining an understanding of how management is monitoring risks that affect their enterprise. The rating agency believes that learning about management's approach to overseeing enterprise- wide risks provides better insights about management's effectiveness. Knowledge about an entity's risk oversight activities will enhance S&P's analytical process and focus, will help better differentiate more effective management, will provide better insights about management, which in turn will create more forward-looking ratings. While ERM is relevant to many stakeholders, S&P's primary interest is on evaluating how an entity's ERM process helps a company repay its financial obligations. Other benefits of ERM are not the focus of S&P.

Economic events of the past year underscore the need for better risk oversight for entities of all types

Primary Focus

S&P's implementation of the ERM evaluation process is being conducted in two stages. In the first year (2008 – early 2009), S&P has been primarily gathering information from entities about how ERM is being done in their organizations. That is, analysts are primarily listening to management's description of how they go about risk oversight and the analysts are then compiling that information to get a sense for the state of ERM in non-financial companies today. In year two (mid-2009 and onward), S&P is working towards publishing the criteria that it will use going forward to actually score the effectiveness of an entity's ERM processes.

Characteristics of Risk Oversight

The primary focus of S&P is to obtain a sense for the substance of management's approach to overseeing enterprise-wide risks. They are examining whether management

- Has an approach to attend to key risks (e.g., is it an intentional versus "drifting" activity)
- Makes conscious decisions about which risks to take (e.g., are decisions made in context with a known risk appetite)
- Knows the entity's risk tolerance (e.g., how does the company communicate what it does and does not want to do)
- Knows what can go wrong with its operations and strategy and has a "Plan B" (e.g., is there an ability to respond to possible events)
- Avoids outsized risks (e.g., avoids "really big risks")
- Is resilient (e.g., has some capacity to bear risks)

S&P acknowledges that there is no one-size-fits-all approach to ERM. Dreyer emphasized that S&P believes there are many different ways to demonstrate risk oversight effectiveness.

Dreyer also emphasized that S&P is not looking for an entity to have a system in place designed to eliminate all risks. It also is trying to focus on the substance versus form of risk oversight. Thus, a system that resembles the cramming together of disparate risk management activities or a system whose focus is merely compliance or disclosure oriented, is not viewed as substantively effective. Similarly, the decision to acquire or develop new software or to appoint a chief risk officer doesn't necessarily signal that the entity's ERM processes are robust.

Emphasis on Culture and Strategy

Analysts will primarily focus on two primary elements of risk oversight: culture and strategic risk management

As S&P conducts these reviews, its analysts will primarily focus on two primary elements of risk oversight: culture and strategic risk management. The focus on culture will primarily involve assessments of how management's risk oversight processes encourage communications about risks and how management has assigned and communicated roles, policies, metrics, and frameworks throughout the organization. They are interested in understanding the "influence" of risk oversight in day-to-day decision-making.

The focus on strategy will primarily assess how risk-thinking is embedded in strategic planning. More specifically, S&P will try to determine and evaluate how risk oversight processes impact key strategic decisions. Analysts will attempt to gather an understanding of the strategic planning process to determine how risk considerations are integrated and whether the process leads to the consideration of alternative strategies as the risk landscape evolves..

Linkage of Risk and Return

A core business tenet emphasizes the linkage between risks and return: higher returns are generally correlated with greater risks. As part of S&P's evaluations, they are keenly interested in understanding where management wants to be along the curve depicting the intersection of risk and return. They are interested in gaining an understanding of how management tracks where they are along the risk/return curve and whether their return goals are placing the entity beyond its risk tolerances. The analysts are trying to obtain a sense for management's goals for returns and their knowledge and understanding of risks required to generate those returns.

Areas of Interest

As S&P gathers information to aid them in their ERM evaluations, they are entering into discussions and dialogue with management about these issues:

- 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 would your company respond to … (a hypothetical scenario)?

As they engage in these discussions, S&P is looking for evidence of management's risk oversight effectiveness.

For more detailed information, visit S&P's website: www.erm.standardandpoors.com

NYSE Perspectives on Governance and Risk Management

Glenn Tyranski, NYSE Regulation
March 2009 ERM Roundtable

Glenn W. Tyranski, the Senior Vice President of Financial Compliance at New York Stock Exchange (NYSE) Regulation, spoke at the March 2009 ERM Roundtable on the evolving roles of NYSE Regulation and emerging issues surrounding current economic conditions, corporate responsibility, and risk assessment. The NYSE, through a merger with Euronext in 2007 and other investments and strategic alliances over the last decade, is encompassing a more global footprint and has greatly consolidated trading. NYSE Euronext is now a public company with its registrants comprising a global market capitalization of over USD 15 trillion.

NYSE Regulation

NYSE Regulation is a not-for-profit subsidiary of NYSE, with a separate board and senior management that arose five years ago to provide a focus on oversight challenges. NYSE Regulation is comprised of three divisions: Market Surveillance, Listed Company Compliance, and Enforcement. NYSE Regulation is entrusted with the development and oversight of listing standards and has established stringent financial listing requirements and corporate governance standards. The work of NYSE Regulation is overseen by the Securities and Exchange Commission (SEC) and the NYSE's Listing and Compliance Committee. NYSE Regulation is responsible for acquiring new exchange listings, working with continued listings, and public policy and works with many other organizations such as the SEC, the Public Company Accounting Oversight Board, the Financial Accounting Standards Board (FASB), and the International Accounting Standards Board in fulfilling these responsibilities.

The recent marketplace has been slow for new listings and there have been large swings in the NYSE over short periods of time that can be tied to many factors from company-specific to an evolving regulatory environment. The NYSE is currently experiencing record levels of noncompliance with listing requirements that have not been seen since 2000–2001. There is currently a 3% noncompliance rate on the exchange, with a 16% noncompliance rate for "penny stocks" that typically trade for under $5 per share. However, other markets have experienced noncompliance rates exceeding 50% so NYSE listings are still very compliant from a global perspective. In 2008, there were 54 delistings and 66 new listings, significantly down from an average of 300 in many years. Because of this decline, year-to-year global IPO proceeds were down 68%. One significant difference in the current downturn from that of 2001 is that the current downturn is not limited to one industry, but is affecting the market as a whole.

Current Economic Conditions

Much of the current problem stemmed from unrealistically low perceptions of risk and excessive liquidity

With the economy in its current condition, consumer confidence levels are at all-time lows and home prices have seen sixteen months of continuous decline. Much of the current problem stemmed from unrealistically low perceptions of risk and excessive liquidity. Risk models did not account for the effects of significant declines in liquidity like those that have occurred, so there was excessive risk-taking in the marketplace. The mortgage business changed from an originate-to-hold model to an originate-to-distribute model. Financial institutions especially have felt the effects of this period of ineffective risk management, oversight, and foresight. In looking at how the economy arrived at its current point, many are asking where the regulation was and criticizing the adequacy of due diligence and curiosity applied. One common denominator for many companies in their current condition is that they had too much debt or, now, lack the ability to access debt.

The past several years have also seen a dramatic shift in trading, with large increases in over-the-counter derivatives and swaps. This resulted in unbundling risk and decreasing risk in some ways by sharing it across many organizations, but at the same time the absolute amount of risk was greatly increasing. The increase in derivatives trading also resulted in large amounts of paper assets and liabilities building up on organizations' books while the derivatives remained unsettled. Then, in a time of distress, settling started to occur, drastically changing the financial condition of many organizations.

Solutions to our current economic state will need to be global. It is difficult to regulate when there is panic in the marketplace and some at least partially blame the absence of regulations against short-selling on the panic. Many are currently calling for the return of the uptick rule that has been absent since 2007. However, it bears keeping in mind that problems have not only occurred due to short sales, but there have also been long-term holders unwinding positions that causes problems for thinly-traded stocks.

Corporate Responsibility

In recovering and learning from challenging market conditions, business leaders must work to restore credibility by reaching new levels of transparency and accountability. Management also needs to recognize that, while shareholders are significant stakeholders and earnings are therefore important, there are other objectives for which, and stakeholders to whom, a company is responsible. With improvements in areas such as disclosure, the government's position as a shareholder in many corporations can be relatively short-lived.

In response to these issues of corporate responsibility, the SEC is taking a closer look at board oversight and the risk management responsibilities of the board. The roles and duties of boards are changing as well. Boards that historically have adopted advisory roles, are now expected to also serve monitoring roles, set an effective tone-at-the-top, and be proactive in dealing with issues facing their companies.

Risk Assessment

While risk assessment was viewed as important before, the ability for sweeping changes to occur quickly and on a global scale has heightened the importance of risk assessment. There are several ways in which poorly developed risk assessment strategies contributed to recent market problems. These shortfalls included a too-strong focus on the short-term, boards providing minimal oversight, risk managers operating in vacuums, and overreliance on risk models.

In moving forward, there are many areas in which risk assessment can be strengthened in organizations. Risk assessment frameworks need to be strong enough to support business goals and risk assessment needs to permeate and be sufficiently communicated throughout the organization. Risk management is an ongoing process and involves identifying, tracking, and managing, not controlling, risks. Risk should be a regular agenda item for boards. Finally, organizations need to remember that there is more than just credit risk; there are also market risks, reputation risks, and others that should be of concern.

Shortfalls included too much of a short-term perspective, boards not exercising enough oversight, risk managers operating in vacuums, and overreliance on risk models

Companies throughout the market need to remember not to lose sight of long-term issues just because there are short-term issues requiring immediate attention. In recent years, many companies failed to contemplate systemic risk and a culture of excessive risk-taking was tolerated. Now, the pendulum has swung, and the current climate is very risk-averse. One benefit from the downturn we are experiencing is that there is increased thinking about risks versus rewards in making business decisions that will hopefully continue as the markets improve.

Importance of Culture and Judgment in ERM

David Fox, KBR, Inc.
April 2009 ERM Roundtable

David Fox, the Director of Risk Management at KBR, Inc., based in Houston, Texas, spoke about the rollout of ERM at KBR and its evolving role in the company. He emphasized the importance of culture and the need for communication and judgment for risk oversight to be effective and sustainable.

About KBR

While part of the larger Halliburton, Inc. organization for many years, KBR, Inc. officially became an independent company in April 2007. KBR is a Houston-based leading global engineering, construction and services company supporting the energy, petrochemicals, government services and civil infrastructure sectors. With revenues exceeding $11 billion, this New York Stock Exchange registered company is comprised of six business units with operations around the world. This diverse operational and geographic presence along with its infancy as a stand-alone company gave KBR the potential to realize significant benefits from ERM implementation.

KBR's Rollout of ERM

The approach to implementing and facilitating ERM at KBR comes from the perspective of having a primary goal of trying to promote a conversation about risk among senior management and the board. The ERM effort started in 2007 with a desire by KBR to be best-in-class at risk awareness. This has evolved over the past two years so that KBR's current focus is on best-in-class risk awareness as well as expert and timely perspectives about emerging and strategic issues.

Fox stressed the importance of tone at the top in implementing ERM at an organization. KBR has strong support for ERM from executive management and the board of directors, which helps to create a culture in the organization that is accepting of ERM. Executive buy-in also helps in gaining the necessary support from others within the organization who may be resistant to change. ERM's importance at KBR is evident as their desire for best-in-class risk awareness is one of the key values identified in the mission, vision, and values of the company.

The first step in implementing ERM was to develop an ERM strategy, which was done in collaboration with the internal audit and financial controls functions. The next step was then to identify the risks facing KBR. In July 2007, and then annually thereafter, an ERM survey was sent out with about sixty questions, asking people to assess the impact and likelihood of different risks based on their cumulative effect on profits or cash flows over the following three years. These assessments were made based on the controls that were currently in place in the organization. Structure was provided to assist in providing some consistency in the assessments of risk probability and risk impact. The impact scale was from 1, significant, to 5, catastrophic, and the likelihood scale was also from 1, highly improbable, to 5, probable.

Alignment of risks through dialogue and discussions among management helped to gain a more unified perspective on risk across the company

After risks had been identified, they were assessed using a heat map reflecting the rank-ordering of risks based on the survey responses. Risks were assessed by executive management, senior management, and business unit management, and groups would often rate risks differently. Furthermore, individuals within each group often rated risks very differently as well. Alignment of risks through dialogue and discussions among management helped to gain a more unified perspective on risk across the company and helped individuals and groups to gain an understanding across functions about the risks seen by other functions.

Fox believes the most effective way to implement ERM is by using tools already in place in the company and by packaging and promoting all corporate risk management processes, including responsibilities in different groups, into one risk narrative. KBR already has strong governance, compliance, and quality, health, safety, and environment processes in place that provide the foundation for its ERM program. KBR's Project Risk Management Group provides existing tools that analyze projects using a risk breakdown structure, risk register, and risk management system.

KBR also has a Business Development Oversight (BDO) Group that looks across all projects to facilitate greater risk awareness, provide a portfolio view of risk and return, and ensure smooth handovers from sales to operations. BDO actually looks at the commercial, execution, financial, and contractual risks of each project to build a risk premium into the price of every deal. The ERM program then builds on all of these existing processes to look forward with a multi-year view to consider risks that will affect KBR as a whole, probing the periphery in an effort to detect early indicators of impending threats or potential opportunities. Thus, ERM acts as an instrument to try and discover emerging risks and increase the awareness of those risks across the company.

Lessons Learned

Based on his experiences in the first few years of implementing ERM at KBR, Fox shared several lessons learned. Simplicity is a key to being able to further ERM efforts in an organization. The ERM process should involve familiar tools, presentations should be designed to promote dialogue, and the ERM effort itself should avoid using a lot of resources. ERM should be approached from a qualitative perspective, concerned with socialization and probing for emerging risks, not metrics.

ERM should also be part of a separate effort and conversation whenever possible instead of an add-on as part of another effort or meeting. Finally, time horizon should be considered as agility is important and there should be a pipeline in place to surface immediate concerns. The time horizon also needs to be matched with the orientation of the audience, talking about more strategic issues with the board of directors and more operational issues with management. By following these approaches, ERM will have the chance to evolve slowly through an organization, and through this evolution a buy-in and understanding of the processes necessary to keep ERM going will also develop.

NC State University ERM Initiative - Vision, Mission, & Purpose

The ERM Initiative at North Carolina State University is pioneering thought-leadership about the emergent discipline of enterprise risk management, with a particular focus on the integration of ERM in strategy planning and governance. The ERM Initiative conducts outreach to business professionals through executive education and its internet portal (www.erm.ncsu.edu); research, advancing knowledge and understanding of ERM issues; and undergraduate and graduate business education for the next generation of business executives. The ERM Initiative has a

Vision
To be internationally recognized as an ERM thought leader.

Mission
To be a national and international thought leader in enterprise risk management (ERM) and in the implementation of ERM in strategy development and corporate governance.

Purpose
To pioneer the development of this emergent discipline through outreach to business professionals, with our ongoing ERM Roundtable Series and internet portal; research, advancing knowledge and understanding of ERM issues; and undergraduate and graduate business education for the next generation of business executives.

ERM Initiative Resource Center

As boards of directors and senior executives seek to implement an enterprise-wide view of risk management, they benefit from best practices developed by many ERM thought leaders. Often these resources provide practical insights about effective techniques for effective ERM, including case study examples. The ERM Initiative has compiled summaries and abstracts of over 150 ERM-related publications, which are presented on our website, www.erm.ncsu.edu.

For more information, contact the ERM Initiative:

ERM Initiative
Box 8113
College of Management
North Carolina State University
Raleigh, NC 27695-8113
919.513.0901
ERM_Initiative@ncsu.edu