

Enterprise Risk Management: A Renewed Focus

World Energy® interviews

*David M. Johnson, Managing Director of Energy & Utilities, and
James DeLoach, Managing Director of Governance, Protiviti*

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) recently released the Integrated Framework for Enterprise Risk Management (ERM) with the intent of helping organizations to improve their capability to manage risks across their enterprise. The energy sector touched on aspects of this concept a few years ago, but in light of some of the problems in recent years, there is a renewed focus to proactively assess risk across the enterprise.

World Energy: How long has ERM been around and why has there been a renewed focus on it?

DeLoach: The concepts and theories underlying ERM, namely a portfolio view of risk, have been around a long time. The application of these concepts and theories has emerged in financial institutions and world-class corporate treasuries as they apply at-risk frameworks, capital attribution technologies and other measurement methodologies to the management of market risk and credit risk. However, market developments over recent years have made it clear that volatility isn't just a currency, interest-rate or equity security risk anymore.

Customer preferences, competitor product offerings, labor markets and technology are all changing with increasing frequency, with their behavior resembling that of the financial markets. Even the life cycles of organizational business models are compressing. Change is no longer linear, but exponential. Successful companies must innovate and deliver total solutions that create new sources of value for their customers or markets or they will lose ground to nimbler, more creative rivals. This way of thinking makes business strategy a fluent, dynamic process. Risk management augments that process.

For most companies, however, the chasm between the traditional risk management model and ERM was simply too overwhelming. Therefore, in recent years, ERM has been pursued more by visionary organizations than by the mainstream.

World Energy: Has Sarbanes-Oxley had an impact on ERM?

DeLoach: Compliance with the Sarbanes-Oxley Act laid a foundation for implementing ERM capabilities that did not previously exist. Companies that have implemented improved disclosure processes and internal control over financial reporting should take a closer look at how they can expand these capabilities to encompass all business activities, because

the chasm is not as great as it once was due to the ongoing compliance effort required by Sarbanes-Oxley.

World Energy: What is the value proposition for implementing enterprise risk management?

Johnson: ERM redefines the value proposition of risk management by providing firms the processes and tools they need to become more anticipatory and effective at evaluating, embracing and managing the uncertainties they face as they create sustainable value for stakeholders. ERM helps a company manage its risks to create and protect value in three ways. First, it helps establish a sustainable competitive advantage. Second, it optimizes the cost of managing risk. And third, it helps management improve business performance. These contributions redefine the value proposition of risk management to a business. They elevate risk management capabilities to a strategic level.

These valued-added contributions from ERM lead to possibly the greatest single benefit that risk management can make to the success of a business: that is, to instill greater confidence in the board, CEO and executive management that risks and opportunities are being systematically identified, rigorously analyzed and exploited on an enterprise-wide basis consistent with the enterprise's risk appetite and business model for creating and protecting value.

World Energy: Why would a public company take on ERM on the heels of Section 404 compliance?

DeLoach: ERM supports and builds on Sarbanes-Oxley compliance efforts. Section 404 compliance requires the implementation of an ongoing process to address financial reporting risk. Because most companies are using the COSO Internal Control-Integrated Framework as criteria for complying with Section 404, many elements of the compliance process

also apply to the implementation of ERM. Therefore, Section 404 provides a foundation for implementing ERM.

While ERM can enhance the quality of internal and external reporting, integrity in reporting is a prerequisite for, not a result of, ERM. A full and honest commitment to truthful reporting, which is a goal of Sarbanes-Oxley, surfaces the vital signs of change, which management must consider when evaluating whether strategies and objectives remain market-facing, customer-focused and competitive. An organization cannot manage its risks when it suppresses information about business realities.

While ERM focuses on business risk and internal controls with an objective to preserve as well as create enterprise value, it also aligns strategy, people, processes, technology and knowledge. The emphasis is on strategy. And the application is enterprise-wide. By managing risks strategically across the enterprise, an organization not only supports Sarbanes-Oxley compliance but also brings to light new risks as they emerge. Transparency is the name of the game. While there is no question the disclosure process is vital, so too is the process of managing other risks. ERM instills the discipline needed to continuously improve risk management capabilities.

World Energy: Are companies implementing ERM?

Johnson: ERM is a best-of-breed approach that different companies apply in different ways. Most companies are applying the traditional risk-management model in their business, which makes ERM a “future-state goal.”

The evolution from the traditional risk management model to ERM is not easy. Under traditional risk management approaches, the focus is fragmented, risk is a negative, reactive and ad hoc behavior is acceptable, and the risk management activity itself is transaction oriented (or cost based), narrowly focused and functionally driven. The traditional model is focused on managing uncertainties around physical and financial assets. Under ERM, proactive behavior is expected, and the risk management activity is continuous, value based, broadly focused and process driven. ERM is focused on the enterprise’s entire asset portfolio, including intangibles such as customer assets, employee assets and supplier assets. The process also pinpoints organizational assets such as differentiating strategies, distinctive brands and innovative processes and systems.

Very few companies have implemented a true enterprise-wide approach in all aspects of the business. Companies at the early stages of developing their ERM process often lay a foundation with a common language, a risk management oversight structure and an enterprise-wide risk assessment process. A few companies have evolved toward more advanced stages, such as institutions in the financial services industry managing market and credit risks. Some companies apply ERM in specific units, such as in a trading unit.

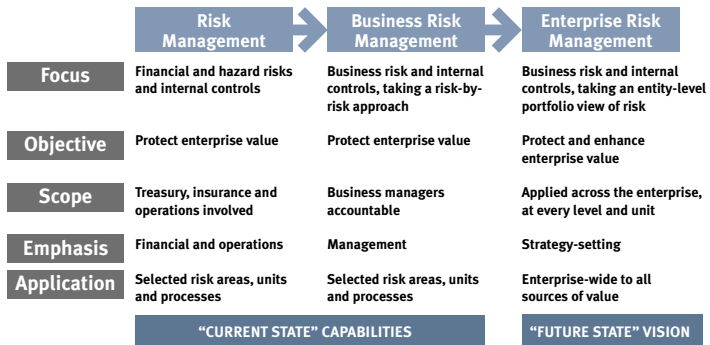
World Energy: Is there any way to benchmark the level of investment required to implement ERM?

DeLoach: One effective way to determine the level of investment is to compare the organization’s existing risk management to a framework (such as the COSO framework) and, using that comparison as a context, empower a group of senior executives to define the role of risk management in the organization. Based on this assessment, the level of investment can be priced based on the people, tools and other resources required.

COSO states that ERM “is effected by an entity’s board of directors, management and other personnel.” It is integral to what they do. Managing an organization and managing risk should be inextricably linked. Therefore, management must decide the nature of the ERM solution based on the organization’s size, objectives, strategy, structure, culture, management style, risk profile, existing infrastructure, industry, competitive environment and financial wherewithal. Another important factor involves an understanding of the enterprise’s critical risks and the capabilities around managing those risks. The bottom line for most companies is that they will find the value proposition of ERM infrastructure more compelling if there are significant gaps in their capabilities around managing their critical risks.

World Energy: Don’t successfully run companies already do this?

Johnson: We would expect that successfully run companies are applying many aspects of ERM. It is indeed difficult to succeed without identifying, formally assessing, responding to, controlling and monitoring risk. However, we suggest that few companies on the planet can say with certainty their risk management practices need no further improvement. The message is not about what companies are currently doing, but about what companies must do to determine whether they can enhance or improve their capabilities.



Today, there are continually changing profiles of risks that have not only financial implications, but strategic and operational impacts as well. As executives examine the risks their companies face today, they will see a different profile from what they saw even a few years ago. And, more importantly, they can expect to see even different risks just a few years from now.

World Energy: Does ERM apply to every organization?

DeLoach: Every organization faces risk. ERM is a process for dealing with risks and opportunities. Executive management in most organizations is focused on investment and return, on opportunity and reward and on competitive advantage and growth. That's why ERM is vital to success as it assists managers in gaining the confidence that they understand their risks and the capabilities to manage those risks, invigorating opportunity-seeking behavior.

Every organization takes risk. Every choice management makes to act or not to act affects the organization's risk profile. ERM can assist management in developing a differentiating skill in selecting the best bets for a company to take, given the competitive and regulatory forces in the external environment.

Every organization responds to risk. CEOs and their management teams must enable and motivate their organizations to capitalize on changing opportunities. They must continually invest scarce resources in the pursuit of promising – though uncertain – business activities. They must manage existing business activities in the face of changing circumstances. And, as they do all of these things, they must simultaneously be in a position to confidently assure investors and other stakeholders that their organization is effectively managing risk while thriving in the global marketplace. As if that isn't enough, in the face of Sarbanes-Oxley, the chief executive officer and the chief financial officer must be champions of transparent public reporting.

ERM will help executives and directors meet these challenges.

World Energy: How should the board be engaged in the ERM process?

DeLoach: When it comes to management, the board wants answers to questions like, What are your critical risks and how are they managed? When there are significant changes in the underlying risks the organization faces, are you informing the board in a timely manner? The best way to engage the board is through information. Executive management needs information to make decisions confidently regarding the risks the company faces and the value proposition for the enterprise as a whole in taking those risks.

World Energy: Can you give a few examples of that kind of information?

DeLoach: You can start with a summary of the top risks for the enterprise as a whole, broken down by operating unit, geographic location or product group. Or a summary of the top and worst performing investments and reasons why.

You might summarize the exceptions versus policies or established limits that have been encountered, including any significant breakdowns, errors, accidents, losses (as well as lost opportunities) or "close calls." Then there are special studies or targeted analyses to evaluate questions about specific events or anticipated concerns that could "stop the show" – for example, what is our Latin American or Asian exposure?

Finally, you could summarize the sensitivity and scenario analyses evaluating the impact of changes on such key variables as interest rates, exchange rates, inflation, weather, competitor acts and supplier performance levels. All these factors are beyond management's control with respect to earnings, cash flow, capital and the business plan.

World Energy: How should the board exercise oversight over the implementation of ERM?

Johnson: Just as a company needs a process to procure quality materials at a competitive cost from its suppliers, it needs a process to manage and reduce its risks to an acceptable level. Without a process, risk management is an ad hoc, reactive activity that is fragmented across the enterprise. ERM provides an alternative – a holistic process view – leading to risk management capabilities that are repetitive, defined and managed. ERM can assist the board in understanding management's risk-taking decisions and in creating confidence that management is reporting relevant information to the board on a timely basis.

Anticipatory and proactive oversight requires a strong emphasis on up-front board involvement in policy setting, risk assessment and strategy formulation. Boards enhance the quality of the oversight process by adding value to management's assessment of the organization's risks. Once risks are identified and sourced, boards should assist management with evaluating the company's options for managing the organization's critical risks, leading to policies clarifying responsibilities, authorities and accountabilities.

World Energy: What questions might directors ask about ERM?

DeLoach: Regarding strategy, a director might ask if management involves the board in a timely way during the strategy formulation process, including when decisions are made to accept or reject risk.

Directors may also want to know if a company is taking significant risks that the board does not understand. For example, if an operating unit or product group is earning superior returns relative to competitors, is it due to taking significantly greater risks than competitors? Are the critical risks inherent in our business model fully understood and managed by people with the requisite knowledge, skills, tools and information? How do you know?

There are other strategy questions: Does the board understand the priority business risks and how those risks are addressed? Are the risks on a list? Is there sufficient time during board meetings to discuss these risks?

World Energy: Are there specific questions about policy?

Johnson: Yes. The directors would want to know how management encourages and rewards growth and innovation without creating unacceptable exposure to risk. Are there defined boundaries and limits that clearly specify behaviors that are off-strategy and off-limits?

At the same time, are entrepreneurial activities and the control activities of the business in balance so that neither is disproportionately strong relative to the other? Are the risks inherent in opportunity-seeking behavior understood and managed? How do you know?

And the directors will want to know about execution. For instance, does management understand the uncertainties inherent in its strategies for achieving business objectives and performance goals? How do you know?

Are there adequate assurances that risk responses and the related control capabilities and information and communication processes are operating effectively? How do you know?

Are contingency plans in place to respond in the event of a crisis? How do you know? Is there an early warning system or executive team dashboard for "mission-critical" risks?

Are there effective processes in place to continuously identify risk, measure its impact and evaluate risk mitigation capabilities? Again, how do you know?

Finally, there could be questions about transparency. Directors may ask about the processes for reliably reporting on risk and risk-management performance. Ideally, the company should have an organizational structure in place that supports the risk management reporting process – and be able to explain how it works.

World Energy: Why this focus on risk management?

DeLoach: The board's purpose regarding risk management is to understand the risks that their organizations face and determine whether the entity has the appropriate strategies and the needed capabilities to manage those risks. The ERM framework provides an excellent tool for directors to use to direct their oversight activities with respect to risk management. This is an evaluation that should take place at least annually.

Protiviti is a leading international provider of independent internal audit and business and technology risk consulting services. Protiviti helps companies worldwide identify, measure and manage operational and technology risks they face within their industries through systems and processes. The firm also offers a full spectrum of internal audit services, technologies and skills for business risk management. Protiviti is a highly respected expert in assisting companies with corporate governance, and our professionals have extensive experience in assisting clients with enterprise risk management (ERM) initiatives in many different industries.

For further information, contact:

David M. Johnson
Managing Director –
Energy & Utilities

James DeLoach
Managing Director –
Governance

david.johnson@protiviti.com

jim.deloach@protiviti.com

Or visit www.protiviti.com