EMERGING BEST PRACTICES in Developing Key Risk Indicators and ERM Reporting

AN EXECUTIVE WHITE PAPER
BY JAMES LAM & ASSOCIATES

SPONSORED BY
COGNOS, AN IBM COMPANY

JAMES & LAM ASSOCIATES

COGNOS®
AN IBM® COMPANY

This edition published January 2008

Table of Contents

"It would be a mistake to conclude that the only way to succeed in banking is through ever-greater size and diversity. Indeed, better risk management may be the only truly necessary element of success in banking."

Alan Greenspan
Chairman of the Federal Reserve
American Bankers Association Annual Convention
October 5, 2004

The level of interest in risk management has never been greater among corporate executives, financial analysts, and regulators. While it has long been recognized as a core competence in banking, risk management has gained recognition as a critical management discipline in other risk-intensive industries, including securities brokerage, asset management, insurance, energy, and large multinational corporations. The interest in risk management extends all the way to the boardroom. According to a 2005 McKinsey & Company survey of 1,000 board members, 76 percent would like to spend more time on strategy and risk management. However, the level of risk transparency at the board level is lacking. The same survey indicated that only 8% of directors had a complete understanding of key risks in the long-term strategy for their company, while 37% had no or limited understanding.

More importantly, the practice of risk management has shifted in a fundamental way. In the past, companies managed risks by "silos," in which different types of risk—strategic, business, credit, market, operational—were managed by different organizational units. Over time, risk management professionals recognized that risks, by their nature, are highly interdependent. In fact, major corporate disasters are often caused not by a single risk factor but a convergence of risk factors. This recognition has led to the development and implementation of integrated approaches to measuring and managing risks across the enterprise, also known as enterprise risk management or ERM. A March 2005 survey of global companies by the Corporate Executive Board indicated that an overwhelming 91 percent have established (11 percent), or are in the process of establishing (80 percent), an ERM program.

ERM – Key Drivers and Trends

Why are companies adopting an ERM approach? Currently, there are four key forces driving the growth in, and acceptance of, ERM:

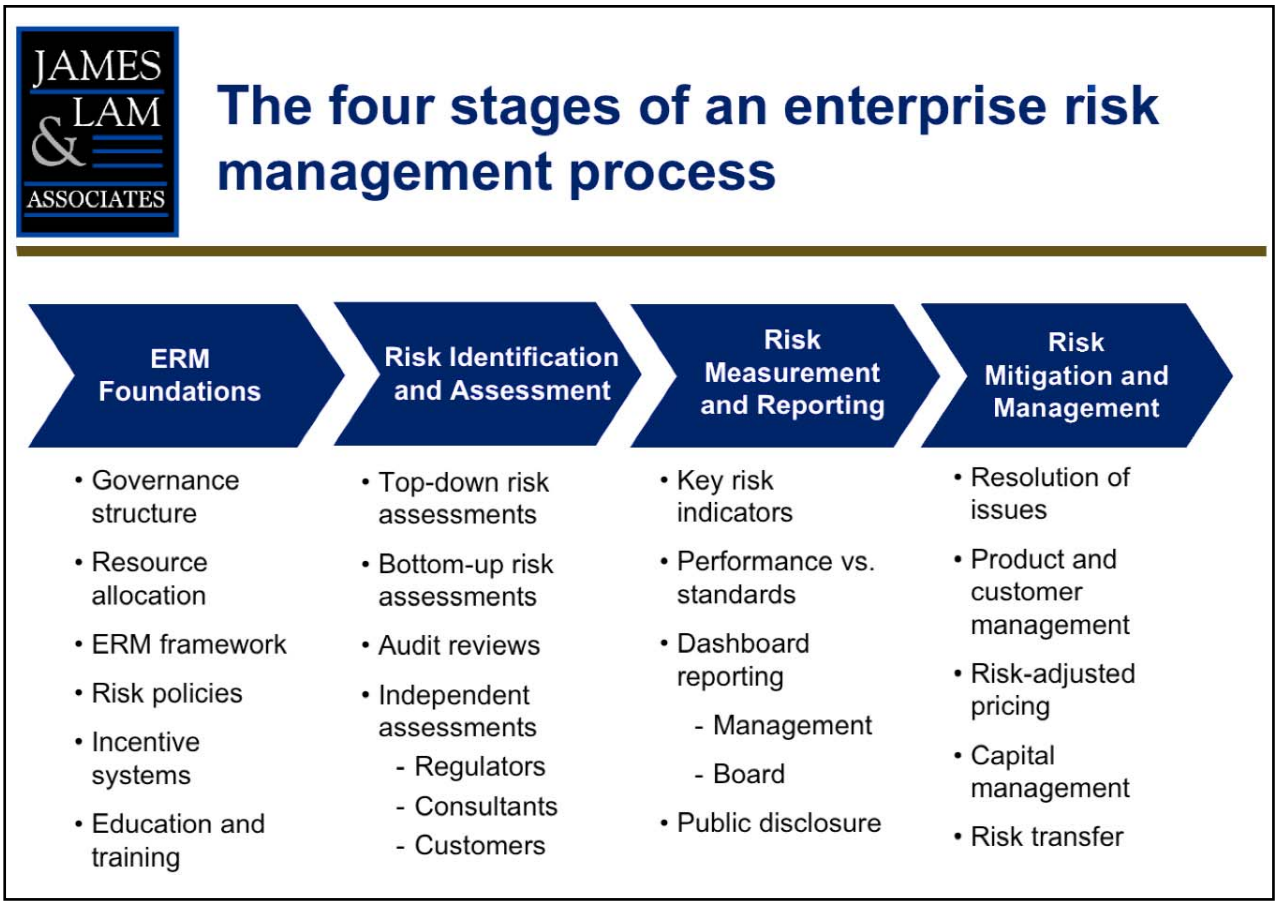
- **Wake-up calls from corporate disasters.** More than ever, board members and corporate executives realize the consequences of ineffective risk management. Notable disasters include companies such as Enron and WorldCom, as well as industry-wide problems such as market-timing and late-trading in the mutual funds industry and bid-rigging in the insurance brokerage industry. In the aftermath of these corporate disasters, board members and executives realize that the only alternative to risk management is crisis management, which can do much more damage to a company's financial and reputational assets.
- **New stringent regulatory requirements.** In response to these events, regulators such as the SEC and the Federal Reserve have increased their examination and enforcement standards. The *Sarbanes-Oxley Act* requires enterprise-wide documentation and testing of controls over financial reporting. Amendments to the NYSE listing standards require audit committees to discuss risk monitoring and control activities with internal and external auditors. Basel II and Solvency II will establish a direct linkage between minimum regulatory capital and the underlying credit risk, market risk, and operational risk exposures of banks and insurance companies, respectively. In the new business environment, there are clear incentives for best-practice risk management, while wrongdoers face financial penalties as well as potential criminal charges and jail time.
- **Global initiatives on corporate governance and risk management.** A number of industry initiatives have been organized around the world to establish frameworks and standards for corporate governance and risk management. The *Treadway Report* (United States, 1992) produced the Committee of Sponsoring Organizations (COSO) framework of internal control, while the *Turnbull Report* (United Kingdom, 1999) and the *Dey Report* (Canada, 1994) developed similar guidelines. In September of 2004, the COSO *Enterprise Risk Management – Integrated Framework and Application Techniques* was published. This framework incorporates corporate governance and internal controls as part of an overall ERM structure. These industry initiatives have clearly established the role of the board and senior management in risk management.
- **Early ERM adopters are reporting tangible benefits.** Companies have reported significant benefits from their ERM programs, including stock price improvement, debt-rating upgrades, early warning of risks, loss reduction, and regulatory capital relief. (Appendix A provides selected case studies of companies across different industries that have reported tangible benefits from their ERM programs.) As well, given the significant costs that companies have incurred to comply with Sarbanes-Oxley, there is an opportunity to convert this "compliance cost" into a "business benefit" by implementing an ERM program.

Role of Risk Measurement and Reporting in ERM

One of the key objectives of ERM is to promote risk transparency, both in terms of internal risk reporting and external public disclosure. Establishing a robust risk measurement and reporting system is therefore critical to ERM success. The old adage "what gets measured gets managed" holds true in risk management. The following illustration shows how risk measurement and reporting fits into the overall ERM process.

The implementation of ERM as a management process involves four stages:

- **Stage 1: ERM foundation setting.** In the first stage, a company must establish a sound foundation for the overall ERM program. The board and senior management provide what is often referred to as "tone from the top." This includes developing the ERM framework, allocating sufficient resources, and engaging in risk policy discussions. The company's risk appetite is also clearly defined in risk policies and limits. Education and learning is another key component, which includes training programs and organizational processes that share best practices and lessons learned. To motivate desired behavior, incentive systems should incorporate risk management effectiveness and risk-adjusted profitability measurement.
- **Stage 2: Risk identification and assessment.** An ERM process should integrate various risk assessments to develop a comprehensive inventory. Top-down risk assessments of strategic and business risks can be gathered from the executive team through one-on-one interviews and/or facilitated group discussions. Bottom-up risk assessments of financial and operational risks can be developed through standardized templates or software applications. In addition, risk assessments from independent sources—auditors and regulators—should be incorporated into the overall inventory. Note that the information developed in this stage is largely subjective and qualitative in nature.



- **Stage 3: Risk measurement and reporting.** In this stage, more objective and quantitative information is developed. This information includes key risk indicators (KRIs) for business risk, credit risk, market risk, and operational risk. To evaluate trends and levels, these KRIs are tracked against policy limits (e.g., market and credit risk exposure limits) or performance standards (e.g., tolerance for error rates or system downtime). External data should also be integrated to provide additional context for internal KRIs. External data can include interest rate trends, industry credit default rates, or competitive or industry benchmark data. Finally, risk reporting is provided to management and the board, as well as outside stakeholders through regulatory filings and public documents.
- **Stage 4: Risk mitigation and management.** The most important stage of ERM is risk mitigation and management. This includes resolution of outstanding issues. Moreover, to be a value-added function, ERM must impact decisions that increase the risk-adjusted profitability of the company. ERM applications—including product pricing, customer management, business development, capital management, and risk transfer—integrate risk management and the key drivers of corporate performance. The overall objective is to make more informed business decisions based on risk management. These decisions may include reducing risk limits during stressed market conditions, implementing an exit strategy to minimize losses on a bad investment, or allocating more capital to grow a business with attractive risk-adjusted profitability.

These four stages of the ERM process should not be implemented in a sequential manner for the overall company. A sequential approach in which a company spends the first year establishing the ERM foundation, the second year identifying and assessing risks, and so forth, is both unproductive and cumbersome. For example, some companies spend a year or more in conducting risk assessments before developing KRIs. In the meantime, the qualitative risk assessments cannot be validated with quantitative data, and the task of designing KRIs for hundreds of identified risks and processes is daunting.

Management should instead focus on the company's most critical risks and apply the overall ERM process to them. Another approach is to start with the end, and first determine the types of management decisions and actions that the ERM process must support. From there, management can work backwards and develop the appropriate KRIs and risk reporting, risk assessment processes, and ERM foundation.

Sources and Characteristics of Effective Key Risk Indicators

The development of effective KRIs is a key challenge for most companies. Financial institutions usually have an abundance of credit risk and market risk indicators, but they are challenged in aggregating this data as well as developing operational risk indicators. On the other hand, non-financial institutions may have significant business and quality information, derived from balanced scorecard and quality initiatives, but they are challenged to develop KRIs for financial risk or technology risk. All companies face the challenge of developing leading indicators that can effectively provide early warnings of potential future losses (see the CIBC case study in Appendix A for an example of the value of leading indicators).

While the development of effective KRIs is a significant challenge, there are some readily available sources from which KRIs can be derived. These sources include:

- **Policies and regulations.** Regulations that govern the business activities of the company, as well as the corporate policies and limits established by management and the board, provide useful compliance KRIs. These KRIs may include risk exposures against limits or compliance with regulatory requirements and standards.
- **Strategies and objectives.** The corporate and business strategies established by senior management, and their associated performance metrics, are another good source. Note that performance metrics are designed to measure expected performance, whereas KRIs should be designed to measure downside risk or volatility of performance.
- **Previous losses and incidents.** Many companies have compiled loss/event databases that capture historical losses and incidents. These databases, or even anecdotic evidence, can provide useful input on what processes or events can cause financial or reputational loss. KRIs can then be developed for these processes and events.
- Stakeholder requirements. Beyond regulators, the expectations and requirements of other stakeholders—customers, rating agencies, stock analysts, business partners—can help in the development of KRIs based on variables that are important to these key groups.
- Risk assessments. Risk assessments performed by the company--including audit assessments, control self assessments, and Sarbanes-Oxley tests--can provide valuable input on the business entities, processes, or risks where KRIs are needed.

Given the various sources for KRIs, the objective should be to develop a high-quality set of KRIs, rather than high-quantity. The following are ten key characteristics of effective KRIs:

1. Based on consistent methodologies and standards.
2. Incorporate risk drivers: exposure, probability, severity, and correlation.*
3. Be quantifiable: $, %, or #.
4. Track in time series against standards or limits.
5. Tie to objectives, risk owners, and standard risk categories.
6. Balance of leading and lagging indicators.
7. Be useful in supporting management decisions and actions.
8. Can be benchmarked internally and externally.
9. Timely and cost effective.
10. Simplify risk, without being simplistic.

* Two of the most useful KRIs used in ERM, value-at-risk and economic capital, can incorporate all four risk drivers.

ERM Reporting – Key Questions and Attributes

Over time, a company may develop hundreds or even thousands of KRIs and risk assessments. Then the company faces a different challenge—the development of an effective ERM report. When designing the format and content of an ERM report, and the functionality of an ERM reporting system, it is important to start by looking at the five basic questions that an ERM reporting system should address:

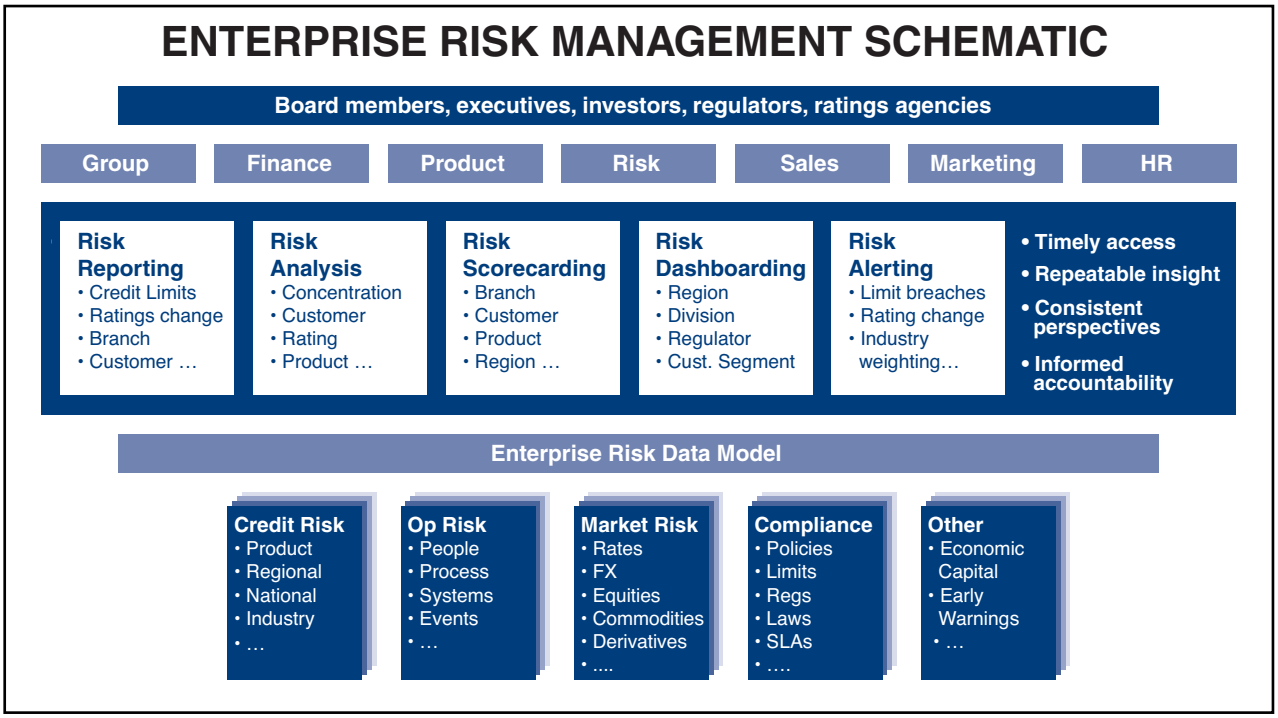
1. Are any of our business objectives at risk?
2. Are we in compliance with policies and regulations?
3. What risk incidents have been escalated?
4. What KRIs and trends require immediate attention?
5. What risk assessments need to be reviewed?

For a typical company, it might take days, weeks, or even months to answer these questions on an enterprise-wide basis. The fundamental problem is that current approaches to risk reporting can be described as "risk measurement by silos," in which management is provided with static reports that provide risk information for different risks separately. Moreover, static reports require significant manual work, resulting in more data problems and less time for risk analysis and strategies.

With an effective ERM reporting system, management should be able to answer all five of these questions in fifteen minutes. An ERM reporting system should provide executive reporting of enterprise-wide risks, and drill-down capabilities so that all key risks can be monitored simultaneously. The key attributes of an ERM reporting system include:

- Provides a single point of access to all critical risk information that may reside in disparate risk systems and data sources.
- Combines executive reporting of enterprise-wide risks with drill-down capabilities to more detailed risk data.
- Delivers "just-in-time" risk information, from real-time risk alerts to monthly credit reports to quarterly risk assessments.
- Integrates quantitative KRIs, qualitative risk assessments, policy documents, and external market data.
- Allows users to provide commentary or analysis to the risk information presented by the ERM reporting system.

The following illustration provides a schematic of an ERM reporting system:



ERM Implementation – Avoiding Common Pitfalls

Early on, the key questions business executives asked about ERM began with *what*. What is enterprise risk management? What are emerging best practices? What are specific industry requirements? Today, the key questions begin with *how*. How to implement an ERM program? How to develop specific ERM tools? How to integrate ERM into business processes?

With respect to ERM implementation, there are five common pitfalls that companies should avoid. These pitfalls, and strategies to overcome them, are as follows:

- ***Don't let the regulatory tail wag the dog – ERM is about management, not simply compliance.*** Companies face an influx of regulatory requirements that they must comply with, such as Sarbanes-Oxley for public traded companies, Basel II for banks, and Solvency II for insurance companies. However, compliance with these and other regulatory requirements represents a necessary but insufficient condition for success. Companies should go beyond compliance and leverage their ERM programs to realize tangible business benefits. For example, Basel II establishes bank regulatory capital requirements only for credit risk, market risk, and operational risk. In addition to these risk categories, leading companies also consider strategic risk and business risk in their capital management frameworks. A more comprehensive capital management framework would enable a company to improve profitability and shareholder value by making better risk-based product pricing, resource allocation, and business development decisions.

- ***Don't just integrate risks – break down organizational silos.*** ERM is not just about integrating the key risks—strategic, business, credit, market, and operational—into a common framework. It is also about breaking down organizational silos in order to identify interdependencies and make trade-off decisions. Most companies have established oversight functions as part of their governance, risk, and compliance activities. These functions generally include risk management, audit, compliance, legal, treasury, and other oversight groups. Leading companies have broken down these silos by establishing organizational structures, processes, and incentives. These initiatives include establishing risk committees at the board and executive levels, appointing chief risk officers, and aligning the interests of individual oversight functions through common objectives, performance measurement, and incentives.

- ***Don't boil the ocean – focus the ERM process on what is most important.*** Given the wide scope of ERM, many companies are overwhelmed with their risk identification, assessment, documentation, and reporting processes. The objective of ERM should not be to address all of the risks faced by the company. In fact, it would be impossible to identify *all* of the company's risks because that list is infinite. The objective of ERM should be to support decisions on the critical risks and opportunities for the board of directors, executive management, and business and operational units. An effective ERM program should prioritize risk information for the company's key decision makers. As such, an indication of ERM success is not to say "We have identified 720 risks across the company, and fully documented related controls and risk assessments," but to say "We have identified the major risks that require the attention of various management groups, and supported their decisions for these major risks." As an example, some companies find it useful to maintain a "top 10 risks" list for the company.

- ***Don't just tell me, show me – quantify risks through effective key risk indicators.*** Many ERM programs produce large volumes of qualitative information (e.g., risk and control assessments, process maps, policies and procedures) that are not conducive to board and management decision making. In order to support policy and business decisions, critical risks must be quantified and reported in a concise and effective manner. That is not to say that quantitative information is more valuable than qualitative data, but there should be a balance in ERM reporting. For the company's most critical risks, quantitative analysis can be used to show trends, risk-adjusted metrics, compliance with policy limits, and performance against established standards. For the same risks, qualitative analysis can be used to provide expert risk assessments, alternative strategies and actions, management recommendations, and other contextual information.

- ***Don't produce volumes of data and reports – develop an ERM dashboard.*** An ERM report should not be a 50-page report that takes the risk committee two hours to simply walk through. A common complaint from board members and senior executives is that they cannot see "the forest from the trees." Companies should develop an ERM dashboard that provides role-based information to key decision makers. During a board or management risk committee meeting, the ERM dashboard would enable board members and senior executives to first see high-level risk information. In addition, it would allow them to drill-down to more granular data if they want to see more details. An exciting possibility is to develop the ERM dashboard so that it not only provides dynamic access to risk information, but also to risk analytical models. As such, it would also enable board members and senior executives to perform real-time scenario analysis, such as "How would a 30% increase in cruel oil price impact our quarterly earnings, as well as market risk and credit risk exposures?" An example of an ERM dashboard is provided below:

Summary

In the past 10 years, technology applications were focused on risk *quantification* in terms of analytical models, such as asset/liability models, VaR models, credit default models, and so forth. Over the next 10 years, technology will focus on risk *communication* in terms of ERM reporting systems. An ERM reporting system will provide board members, corporate executives, and risk professionals with a single point of access to all critical risk information—including objectives-at-risk, early warning indicators, KRIs against policy limits or performance standards, risk assessments and audit findings, escalations of issues and incidents, and risk-adjusted return performance. The time interval for enterprise-wide risk measurement and reporting will move from monthly to weekly to daily, and ultimately to real-time.

The value of risk information is not in its development, but in its application. As such, to realize the full potential of ERM, risk professionals must deliver the right information, to the right decision makers, at the right time.

Appendix A: Case Studies[1]

The following case studies showcase real-life situations where ERM has provided significant and tangible benefits.

JP Morgan Chase

In 1994, JP Morgan Chase received an inexpensive lesson in the need to manage aggregate market risk exposures. Previously, the bank had focused its market risk oversight mainly on its trading businesses. In 1994, the Federal Reserve raised interest rates repeatedly, one result being a significant disruption in the mortgage markets. While the trading businesses performed well, the bank suffered an unexpected, albeit small, loss in a small S&L that it owned.

According to Leslie Daniels-Webster, chief market risk officer, the bank realized from this experience that it needed to manage aggregate market risk exposures across three dimensions—trading portfolios, asset/liability mismatch, and basis risk. The bank further developed its market risk staff and analytical resources, including VaR and stress-testing models. This experience has served the bank well. In 1998, it weathered the Russian crisis, and it reported earnings of $4 billion (up 4.4 percent) while its peers suffered significant earnings declines due to market losses. .

CIBC

In December 1994, the Toronto Stock Exchange published the *Dey Report,* which recommended that the board of every firm listed on the exchange take direct responsibility for risk management efforts within the firm, and report on these efforts in its annual report. At about the same time, CIBC was expanding globally in the capital markets business. So the Canadian bank had both regulatory and business reasons to invest in ERM. That same year, Bob Mark was hired to build an ERM program, including firm-wide market risk, operational risk, and counterparty credit risk.

The ERM initiative paid off four years later. In the middle of 1998, CIBC was concerned with three early warning indicators in the capital markets—widening credit spreads, increasing actual and implied volatility, and the breakdown of historical price relationships. The bank promptly cut global risk limits by one-third prior to the Russian crisis and market drop later that year, thus avoiding significant losses.

Heller Financial

On May 1, 1998, Heller Financial returned to the New York Stock Exchange as a public company. The commercial finance company aimed to be "world class" in its industry, and realized that it needed to establish an ERM program. While Heller was confident in its credit risk and market risk functions, it was missing a formal operational risk methodology and an overall ERM framework.

In September 1999, Mike Litwin, the company's chief credit officer (who was later promoted to chief risk officer) led the development of an operational risk methodology and ERM framework. A critical insight gained during this initiative was that nearly one-third of what Heller had classified as credit losses were in fact operational losses (e.g., inadequate loan documentation). The ERM program was well underway, and then on July 30, 2001, GE Capital announced that it was acquiring Heller for $5.3 billion in a cash transaction, a 48 percent premium. In its press announcement, GE Capital noted that Heller's risk management was one of the company's key assets.

[1] Source: James Lam & Associates, Inc..

Duke Energy

In July 2000, Duke Energy's senior executives gathered for a two-day strategy meeting to discuss the future of the energy business. They reviewed three possible scenarios: "Economic Treadmill" in which U.S. economic growth slips to 1% per year, "Market.com" in which the Internet revolutionalizes the relationships between buyers and sellers, and "Flawed Competition" in which uneven deregulation will continue in the energy industry, resulting in significant price volatility.

To help manage the company's business uncertainty, Duke Energy appointed Richard Osborne as its first CRO earlier that year. As early warning indicators for these three scenarios, management established specific "signposts," including macroeconomic indicators, regulatory trends, technology changes, environmental issues, competitive moves and patterns of consolidation in the energy industry. Today, Duke Energy has performed well relative to its competitors. As of November 2004, the company achieved year-over-year revenue growth of 41percent, compared to 11percent for the industry. The company's stock has increased 45percent in one year, outperforming the S&P 500 by 28 percent.

Rockwell Collins

In July 2001, Rockwell Collins went public. Following the events of 9/11, the supplier of military and commercial aircraft parts faced hundreds of millions in lost sales and the collapse of its commercial market. Yet the company responded quickly and put in place a contingency plan within 10 days. Management credits its ERM program in terms of its preparedness and resiliency.

The company's ERM program had an interesting start. Several years earlier, project manager John-Paul Besong applied ERM to support the implementation of a critical SAP system. The project went so smoothly that he was promoted to chief information officer a short time later. Since that time, ERM has been integrated into other business processes of the company. The results have been impressive. For the company's fiscal year ending September 2004, it reported record sales of $2.9 billion (up 15 percent) and net income of $301 million (up 17 percent). In January 2004, Forbes called Rockwell Collins the best-managed aerospace company in America.

About James Lam & Associates, Inc.

James Lam & Associates, Inc. (JLA) is a consulting firm singularly focused on risk management. JLA has provided consulting and training solutions to leading institutions, including Allied Capital, Bank of China, Citigroup, Federal Home Loan Bank of Chicago, the Federal Reserve, GMAC, OCBC Bank, and the World Bank.

James Lam, President of JLA, is widely considered the first ever "chief risk officer" and an early advocate of enterprise risk management. In a 2005 Euromoney survey, Mr. Lam was nominated by clients and peers as one of the leading risk consultants in the world.

Mr. Lam is the author of "Enterprise Risk Management: From Incentives to Controls," which has ranked #1 best selling among 25,000 risk management titles on Amazon.com. In 1997, Mr. Lam received the inaugural Financial Risk Manager of the Year Award from the Global Association of Risk Professionals. Treasury & Risk Management magazine named him one of the "100 Most Influential People in Finance" two years in a row (2005, 2006).

About Cognos, an IBM company

Cognos, an IBM Company, is the world leader in business intelligence and performance management solutions. It provides world-class enterprise planning and BI software and services to help companies plan, understand and manage financial and operational performance. Cognos was acquired by IBM in February 2008. For more information, visit http://www.cognos.com.

For more information

Visit the Cognos Web site at www.cognos.com

Request a call

To request a call or ask a question, go to www.cognos.com/contactme. A Cognos representative will respond to your enquiry within two business days.

References

Berinato, S., "Risk's Rewards", CIO Magazine, November 2004

Lam, J., and Litwin, MJ. "Where's Risk? EWRM Knows," The RMA Journal, November 2002

Lam, J. "Enterprise Risk Management – From Incentives to Controls," John Wiley & Sons, 2003

Wysochi, B. Jr., "Power Grid: Soft Landing or Hard?" The Wall Street Journal, July 7, 2000

GLOBAL

Cognos ULC
3755 Riverside Drive
P.O. Box 9707, Station T
Ottawa, Ontario
Canada K1G 4K9

ASIA/PACIFIC

Cognos PTY Limited
Level 2 110 Pacific Highway
St. Leonards, NSW 2065
Australia

EUROPE

Cognos Limited
Westerly Point
Market Street
Bracknell, Berkshire
UK RG12 1QB

NORTH AMERICA

Cognos Corporation
15 Wayside Road
Burlington, MA
USA 01803

James Lam
President

James Lam & Associates
Tel: 781.772.1961
Email: jameslam@comcast.net
Web: www.jameslam.com

WWW.COGNOS.COM

(02/08)

COGNOS®
AN IBM® COMPANY