Enterprise Risk Management and Improved Shareholder Value

James R. McDonald and John Rivera

St. Edward's University

Failure of existing risk management strategies for corporations, both private and public, has led to diminished market value, lack of stakeholder confidence, and criminal and civil penalties for senior executive managers and boards of directors. Shareholders, creditors, suppliers/vendors, employees, and governmental regulators, are all demanding that executive management and boards of directors take a more proactive stance for mitigating and managing risk. These demands are occurring across all industries and enterprise sizes, and are not unique to the United States. As a result of these demands, executive management and boards of directors are beginning to use Enterprise Risk Management (ERM) processes and strategies to help manage all risks that could negatively impact corporate stakeholders.

In 2001, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) began to publish its "framework" for understanding and implementing ERM as a set of strategies for managing strategic, financial, and operational risk (COSO, 2005). Corporations are only now beginning to utilize this framework. According to a study of 271 executives interviewed by The Conference Board (Gates & Hexter, 2005), only 11% of publicly traded corporations currently have a formal enterprise risk management program, although over 90% have plans for one.

This article examines ERM as a potent response to the current state of corporate risk management, with a primary focus on Operational Risk Management (ORM). ORM has thus far been underutilized by most enterprises, and yet it holds great promise for managing risk and for protecting shareholder value. It presents an integrated approach to managing operational risk that promises "hard" results from a "soft" strategy to the most difficult areas of operational risk—systems, processes, and people.

ERM Is Encouraged Under Sarbanes-Oxley Act of 2002 (SOA)

The experience of the early 2000s regarding Enron, Worldcom, Tyco, and others, led to significant action by governmental regulatory agencies, in the name of the Sarbanes-Oxley Act of 2002 (SOA) and various state statutes. SOA requires corporate compliance with internal controls and financial reporting and forces changes in the ways corporations function and management behaves. Moeller (2004) believes that effective compliance requires enhanced technical expertise in risk management and enhanced non-technical expertise in business process improvement, internal communications, culture management, and leadership that produces results. It seems clear that SOA is more than controls and reporting. Effective compliance would now seem to require capabilities and systems to assure that all plans, changes, and project rollouts are executed in a manner that ensures performance.

With two years of experience with SOA regulations under their belts, major corporations have faced an average $4.4 million in additional costs of internal staff time plus external consulting expenses, according to Financial

Executives International ("Regulators seek to trim cost," 2005). The Securities and Exchange Commission (SEC) received feedback from industry and has evidence that reports were mostly "check-the-box" formats. A recent SEC Staff Report (SEC, 2005) thus clarified their expectations:

> The desired approach should devote resources to the areas of greatest risk and avoid giving all significant account and related controls equal attention without regard to risk.
>
> [A top-down approach] … requires that management apply in a reasonable manner its cumulative knowledge, experience and judgment to identify the areas of the financial statement that present significant risk … [and] then proceed to identify relevant controls and design appropriate procedures for documentation and testing of those controls. (p.1)

The SEC now explicitly states that compliance must include a top-down, risk-based approach. The SEC expects an ERM strategy that informs and involves all parts of the organization.

ERM Improves Performance and Enhances Shareholder Value

Companies should be able to leverage their initial cost of SOA compliance. Marchetti (2005) suggests that a company may accrue competitive advantage by leveraging their sunk costs by leveraging the knowledge gained through the compliance process; institutionalizing a strong system and culture of internal control and assessing and improving the key business processes identified during compliance. These actions can produce both a thorough and a rational approach to risk management as now required by the SEC. ERM addresses these criteria with a three-part focus on strategic, financial, and operational risk (COSO, 2005).

An enterprise risk management process identifies, assesses, evaluates, and manages priority risks to the organization. The ERM framework was honed by COSO over a four-year period and finalized in 2005. Its framework establishes a working model for applying ERM to all parts of the enterprise, as a practical response to the Section 404 requirements of SOA. Briefly, Section 404 of SOA requires that management assume full responsibility for establishing and maintaining internal control structures and financial reporting. "Section 404 … represents perhaps one of the more important aspects of the Act (SOA)" (Moeller, 2004, p. 104).

COSO emphasizes the following objectives:

- Align the company's risk appetite and strategy,
- Enhance risk-response decisions,
- Reduce operational surprises and losses,
- Identify and manage multiple and cross-enterprise risks,
- Seize opportunities, and
- Improve the deployment of capital.

These objectives suggest a holistic approach as the best method for ensuring compliance and a positive impact on shareholder value. A strategic focus on enterprise-wide risk leads to market advantage and improved return on capital, as well as regulatory compliance.

Few U.S. companies are currently taking an ERM approach; however, three historically regulated industries are developing ERM strategies: the banking, energy, and insurance industries. Most ERM approaches continue to focus primarily on financial risks and regulatory compliance or on specific industry risks, such as safety in construction or health care. There is as yet little emphasis on either strategic risk or operational risk. Many companies admit that their current ERM strategies are little more than "extension(s) of their audit and regulatory compliance processes" (Slywotzky & Drzik, 2005, p. 80). The SEC will continue to press for more thorough efforts for "top-down, risk-based" (SEC, 2005. p. 1) strategies that meet shareholder requirements, as well as regulatory requirements.

Historically, risk management has meant financial controls, surety products, and hedging. SOA and COSO have changed that paradigm to an integrated process that includes financial, strategic, and operational components. Financial risks have typically referred to uncertainty that a corporation will have adequate cash flow to meet its long-term and short-term obligations. Strategic risks have included shifts in technology, brand erosion, or emerging competition (Slywotzky & Drizik, 2005). Operational risks as defined by COSO (2005) must include attention to leadership, business processes, and the culture of the organization. Operational risk is the focus of the remainder of this presentation.

Operational Risk

Operational risk has in the past meant risk associated with a specific business operation (e.g., financial cash controls, or a manufacturing or distribution process). Under Basel II, the Basel Committee on Banking Supervision (2001), however, has defined operation risk with words often quoted in financial articles as "that risk associated with failed systems, processes, and people, or from external events" (p. 2). It is clear that a serious analysis of operational risk must consider not only the risk to business operations, but also to the maturity and effectiveness of key business processes, the capabilities of managers as supervisors, the performance results of individuals and teams, and the effectiveness of all systems that support business process activities. The authors contend that operational risk, as defined under COSO and Basel II is, therefore, a significant and costly source of enterprise risk. It is difficult to measure and to address; nevertheless, doing so holds great potential for improving shareholder value while also meeting regulatory requirements.

People are the only real actors in business, and their acts result in the success or failure of every task, process, decision, plan, or communication. Fraud is not committed by software; mistakes are not made by spreadsheets; and, immature business processes do not become mature by themselves. Operational risk, therefore, resides primarily in the actions taken by people. People must know what to do and how to do it, must desire to do it correctly, and must have a functional process and structure that enables their success. Fitz-Enz (2000) suggested that, since people are the only self-determining assets, it follows that they are the cause of everything that happens. To manage operational risk, human systems must be better managed and human errors must be mitigated. Three tactics for decreasing the effect of human errors are considered: 1) improvement of business processes, 2) installation of management control systems, and 3) improvement of supervisory capabilities.

Managing Operational Risk

Changing a system or process is typically difficult; it upsets the equilibrium of the enterprise and makes people anxious. Hammer (1997) has noted that the history of large change initiatives, such as reengineering, mergers, and enterprise-wide software installations, have often failed to meet expected increases in productivity and shareholder value. Hammer's reversal of his earlier praise for process reengineering is informative (Hammer & Champy, 2001). Hammer and others have concluded that failure to take into account such factors as human needs and motivation when implementing change is largely responsible for the ultimate failures of most reengineering initiatives (Davenport, 1992).

COSO, Basel II, and even the SEC seem to be converging on agreement that an operational risk management approach that addresses human factors such as poor communications and fraudulent behavior holds the promise of minimizing risk, reducing costs, and enhancing shareholder value. COSO's objectives for reducing operational surprises and losses, improving deployment of capital, and making decisions that seize on opportunities, are all aspects of an operational risk strategy. People must be able to collect and analyze the correct information, make good decisions, and work collaboratively with one another. Their decisions then must be communicated clearly. Tasks that are delegated require follow-up to assure that appropriate action was taken and that all individuals with the responsibility to act acted on a timely basis. All links in this value chain rely on human actions, and these human factors hold heavy potential for derailing the objectives. The power of operational risk management, therefore, resides primarily within the business processes and systems that drive mission critical objectives, including the process that drives an ERM strategy itself. Automated tools such as enterprise performance software been helpful; however, people still must make the decisions, communicate those decisions, take the actions required to execute the decisions, and comply with regulations.

Operational Risk Solutions

The business process is the locus of greatest leverage for the elimination of operational risk. Tools and techniques are available to management for reducing that risk, as well as managing individual and organizational resistance to process improvement. A hypothetical organization with no operational risk would have systems, processes, and people that functioned at 100% effectiveness. There would be no process or compliance problems. There would be minimal unwanted turnover, minimal disputes, and minimal litigation. All key performance measures would be on plan. Stock prices would be leaders. The tactics required for operational risk management would help an organization improve business processes, install management controls, and improve supervisory capabilities. These efforts will help to ensure successful planning and implementation of all activities that improve the strategic and operational control of risks. Just as Six-Sigma and ISO 9000 programs have shown the efficacy of targeted business process improvement, improving processes by managing operational risk holds the promise of similar results.

Process improvements imposed by external "experts" or driven down from senior management often result in resistance or outright sabotage. More successful improvements involve "internal experts," those who work the process and know how it could be better. A facilitated intervention ensures that this internal knowledge is utilized as the primary source of best practice improvements. An improved process must also be executed consistently so that responsible managers and employees know what is expected of them and receive clear reinforcement that their actions are on-task. All process participants need correct, timely information; immediate knowledge of priorities and changes; definitions of quality required in their actions and deliverables; and information for addressing nonstandard issues that may arise. Operational risk management, therefore, includes effective management controls to ensure that everyone is doing what management requires. Anthony, Dearden, and Bedford (1984) have recommended that management control systems include an organizational climate focused on results not rules, team accomplishments not individual accomplishments, innovation not strict compliance with procedures, and participative not authoritarian management style. Management controls, therefore, drive behaviors and activities that attempt to control errors and results.

Anti-fraud Cultures

Recent examples of high-level corporate fraud suggest that corruption is often supported by an organization's existing culture (Geriesh, 2003). Studies of cultures generally agree that the tone at the top as set by executives and the board's support of a Code of Conduct are directly responsible for motivating employee behaviors. SOA explicitly recommends the installation and maintenance of ethics programs and holds the board responsible for governing the organization's business ethics and the conduct of the organization in general. The board must oversee the creation of an environment in which the day-to-day behaviors of the management team provide the model for employees to observe and follow. The actions of senior and middle managers reinforce the executive tone, and together these visible models trump any codes or value statements. While attempts to change cultures tend to be difficult and time-consuming, identifying and changing activities and work behaviors can impact a culture over time.

The Coaching Relationship

Processes, controls, and culture are therefore major domains for managing operational risk under an ERM strategy. However, the coaching relationship represents an equally potent opportunity for improving performance by modifying behaviors. The coach possesses experience, skills, and knowledge of company history to help team players connect specific process activities to outcome requirements. The coach also represents authority, with the leverage to assert expectations for a required outcome. Lastly, the coach should demonstrate enough human sensitivity to values, needs, and personal styles that the coaching message will be received without emotional resistance. The research of Blake and Mouton (1986), spanning 40 years, has consistently demonstrated the efficacy of a coach/leader who can demonstrate both concern for production and concern for people, and thus achieve performance through motivation.

Operational Risk Management Tools and Techniques

Corporations have always been motivated to increase productivity, decrease costs, do more with less, and meet short-term goals based on market demands for quarterly performance targets. Global markets, economic shifts, and regulatory compliance are also motivators. Traditionally, operational risk factors have been addressed primarily in skills training (classroom and technology-based) and through systemic change initiatives, such as reengineering, right-sizing, mergers, and new and improved enterprise technology.

These traditional approaches have produced disappointing results. The annual expenditure for corporate training is estimated at around $300 billion according to the Employment Policy Foundation (Hattiangadi, 2000). Although no scientific studies have been found, Fitzpatrick (2001) has reported on the general belief that only 10% of training transfers into the workplace. At the same time, 65%–75% of all major change initiatives fail to meet the expected goals of improved productivity (Hammer, 1997). In part, this has been due to loss of talent and company knowledge when managers and staff leave. Reviews of failed change initiatives (Davenport, 1992; Hammer, 1997) have implicated several causative factors: 1) an inability to communicate with and get buy-in from employees affected by the change; 2) a failure to deal with conflicting characteristics of merged cultures; and, 3) a failure to train and motivate supervisors as expert coaches. These are all human factor issues that fall under operational risk management.

The human resource (HR) function has been the logical driver of performance improvement. However, HR has become more administrative than strategic and has had an uphill struggle, often budgetary, to develop better "soft skill" approaches. The unfortunate legacy of the 1960–70s was that human potential improvements were too touchy-feely for most leaders, and their resistance reinforced a belief that personal needs and values are not to be dealt with in the workplace (Fombrun, Tichy, & Devanna, 1982). The difficulty of measuring performance outcomes with appropriate metrics has also hampered performance improvement efforts.

In spite of this history, methods for managing operational risk are available to management. Performance improvement initiatives can be more successful with performance support software. Orientation and training for performance improvements are more likely to succeed if based on adult learning principles. Used together, these methods provide a potent counter-offensive against immature processes, poor performance, and even outright fraudulent activities.

Software-based Performance Tools

Performance support technology assists workers and managers to do their jobs right the first time, by structuring tasks, work-flow, decision points, controls, information sharing, input requirements, and outputs (Gery, 1991, 1995; Raybould, 1995). This technology has emerged from diverse disciplines such as instructional design, cybernetics, human interface design, cognitive psychology, and software engineering (Gery, 1995). Such tools ensure that each step in a process is controlled; that the information or skills required are available when and where needed; and that best practices are captured for future learning. Performance-centered technology (Raybould, 1995) grew out of the observation that the effort required for learning is always greater than the time available at the moment of need (Gery, 1995). Most people are not consistently motivated on their own to expend the effort required to transfer classroom or web-based learning to the workplace, even when that learning experience is effective. Performance support provides management controls for ensuring that expected outcomes, such as regulatory compliance, are successfully accomplished. It helps to remove human error so that business processes become consistent and predictable. These applications can be constructed from existing software objects and configured to meet the requirements of a particular business and process. Traditional training methods would still be required for improving processes, however, since not all learning is wedded to a specific task.

Adult Learning Methods

Traditional training methodologies continue to produce weak performance improvements. However, learning that is designed and delivered consistent with adult learning principles has a significantly more positive impact on performance. The key principles of adult learning focus on the role of planning, delivery, location, and quality of participant involvement in the learning process (Fritz-Enz, 2000). Three of the most important principles are:

- Contextual learning—job-related learning is most effective when it occurs in the context of the job variables participants experience while performing;
- Situated cognition—learning is most effective when it occurs as close as possible to the actual job situation; and,
- Constructed learning—learners become more engaged in the learning experience when they have input into objectives, best practices, and case materials.

The most productive learning, with the shortest time to competency, occurs through the process of accomplishing real work. Adult learning principles should be used in both orientation events and in the acquisition of new technical skills. These principles become even more critical during time of organizational change, when worker stress is heightened. Change management and new skill development are critical to the success of process improvement for a successful ORM system.

The study of management has produced numerous models for improving performance. The models provide strategies for managers to assess impediments to performance, to ensure that people perform to expectation, and- to raise the probability that that human knowledge and talent will remain with the organization during times of change. All strategies must be used to ensure the effectiveness of process improvements, the development of a culture of accountability and trust, and the interpersonal capabilities of supervisors.

Solution Outcomes

Many business units already possess the combined knowledge and expertise required by any given process for success. Many work groups can agree on appropriate financial and nonfinancial measures of performance success by which to judge their results. However, their work product is often still not consistent because of the difficulties imposed by human dynamics and the maturity level of the process itself. An operational risk management approach can ensure that all parties to a process, including an enterprise risk management process, will perform all process activities effectively and on a timely basis.

Summary

The intent of this article is to raise awareness of enterprise risk management as a strategy for complying with Sarbanes-Oxley requirements and also for improving shareholder value based on improved performance. These two objectives have converged with previously unconnected initiatives driven by SOA, COSO and Basel II in Europe. An operational risk management approach under ERM that requires corporations to comply beyond internal financial controls and reporting is being mandated. Improved business processes, systems, and effective managers are all risk management foci. The costs of compliance already incurred by corporations need to be leveraged. The requirements of SOA, in forcing the identification of all key business processes, provide a springboard for assessing enterprise-wide risk and for designing improvements to business-as-usual that will raise performance and reduce expense. This frontal attack on the difficult-to-manage human factors brings together the best of organizational behavior, technology, management controls, and process improvement. Specifically, performance support tools and adult learning methodologies to address operational risk can now be integrated into a powerful ERM initiative. ERM promises not only by-the-numbers compliance, but also performance results.

References

Anthony, R. N., Dearden, J., & Bedford, N. M. (1984). *Management control systems.* Homewood, IL: Irwin, Inc.

Basel Committee on Banking Supervision. (2001). *Consultation document: Operational risk.* The Bank for International Settlements.

Blake, R. R., & Mouton, J. S. (1986). *Executive achievement: Making it at the top.* New York: McGraw-Hill Book Company.

COSO. (2005). *Enterprise risk management—Integrated framework.* Retrieved February 4, 2005 from http://www.coso.org/audit_shop.htm

Davenport, T. H. (1992). *Process innovation: Reengineering work through information technology.* Boston: Harvard Business School Press.

Fitz-Enz, J. (2000). *The ROI of human capital.* New York: AMA. Retrieved February 4, 2005, from http://www.amanet.org/books/catalog/0814405746_go.html

Fitzpatrick, R. (2001). The strange case of the transfer of training estimate. *The Industrial-Organizational Psychologist.* 39(2). Retrieved September 15, 2005, from http://www.siopo.org/tip/backissues/TipOct01/03fitzpatrick

Fombrun, C. J., Tichy, N. M., & Devanna, M. A. (1982). *Strategic human resource management.* New York: John Wiley & Sons.

Gates, S. & Hexter, E. S. (2005). *From risk management to risk strategy.* New York: Conference Board.

Geriesh, L. (2003). Organizational culture and fraudulent financial reporting. *The CPA Journal.* Retrieved September 1, 2004, from http:www.nysscpa.org/cpajournal/2003/0303/features/f032803.html

Gery, G. (1991). *Electronic performance support systems: How and why to remake the workplace through the strategic application of technology.* Boston, MA: Weingarten Publications.

Gery, G. (1995). Attributes and behavior of performance-centered systems. *Performance Improvement Quarterly,* 8(1), 47-93.

Hammer, M. (1997). *Beyond reengineering: How the process-centered organization is changing our work and our lives.* New York: Collins.

Hammer, M., & Champy, J. (2001). *Reengineering the corporation: A manifesto for business revolution.* New York: HarperBusiness.

Hattiangadi, A. V. (2000). Upgrading workplace skills: Business' $300 billion annual investment. *Contemporary Issues in Employment and Workplace Policy.* Retrieved on November 12, 2005, from http://www.efp.org/pubs/newsletter/2000/ib000410.pdf

Marchetti, A. M. (2005). *Beyond Sarbanes-Oxley compliance: Effective enterprise risk management.* New Jersey: John Wiley and Sons, Inc.

Moeller, R. R. (2004). *Sarbanes-Oxley and the new internal auditing rule.* New Jersey: John Wiley and Sons, Inc.

Raybould, B. (1995). Performance support Engineering: An emerging development methodology for enabling organizational learning. *Performance Improvement Quarterly,* 8(1), 7-22.

Regulators seek to trim cost of rules on auditing. (2005, May 17). *The New York Times.* Retrieved May 21, 2005, from http://www.nytimes.com/2005/05/17/business/17audit.html

SEC. (2005, May 16). *Commission statement on implementation of internal controls reporting requirements.* Retrieved October 15, 2005, from http://www.sec.gov/news/press/2005-74.html

Slywotzky, A., & Drzik, J. (2005). Countering the biggest risk of all. *Harvard Business Review.* 39(2) 78-88.

Biographies

James R. McDonald, PhD, is a cofounder of ValuePoint LLC, a service company focusing on Enterprise Risk Management consulting and support of Sarbanes-Oxley compliance, using Operational Risk Management strategies. Jim has been a management consultant for over 25 years. He is a licensed psychologist and has taught as an adjunct instructor in the MBA program at St. Edward's University.

John Rivera, MBA, is a cofounder of ValuePoint LLC. John has been a senior finance executive for over 30 years with diverse accounting and finance experience at Motorola and Texas Instruments, Inc. He also has international experience leading major finance and accounting teams in Hong Kong, China. John is a Certified Fraud Examiner, and an adjunct instructor in New College at St. Edward's University.