MANAGEMENT

STRATEGY

MEASUREMENT

MANAGEMENT ACCOUNTING GUIDELINE

Identifying, Measuring, and Managing Organizational Risks for Improved Performance

By

Marc J. Epstein

and

Adriana Rejc

Published by:

CMA CANADA

AICPA®

NOTICE TO READERS

The material contained in the Management Accounting Guideline *Identifying, Measuring, and Managing Organizational Risks for Improved Performance* is designed to provide illustrative information with respect to the subject matter covered. It does not establish standards or preferred practices. This material has not been considered or acted upon by any senior technical committees or the board of directors of either the AICPA or the Society of Management Accountants of Canada and does not represent an official opinion or position of either the AICPA or the Society of Management Accountants of Canada.

MANAGEMENT

STRATEGY

MEASUREMENT

MANAGEMENT ACCOUNTING GUIDELINE

Identifying, Measuring, and Managing Organizational Risks for Improved Performance

By

Marc J. Epstein
Rice University and Harvard Business School
and

Adriana Rejc
Faculty of Economics, University of Ljubljana

Published by The Society of Management Accountants of Canada
and The American Institute of Certified Public Accountants

1 2 3 4 5 6 7 8 9 0 PP 0 9 8 7 6 5

ISBN 0-87051-619-1

IDENTIFYING, MEASURING, AND MANAGING ORGANIZATIONAL RISKS FOR IMPROVED PERFORMANCE

INTRODUCTION

The world has changed significantly in the last five years. New and greater pressures and risks have dominated both the international and business news, dramatically altering the issues that corporate managers must address. The attacks of September 11, 2001 made business executives aware that they must take action to prevent acts of terrorism as well as to prepare for their occurrence at the corporate site and in the wider community. The collapse of notable companies such as Enron and WorldCom highlighted the risk of financial fraud, raised new concerns about corporate governance and internal control, and resulted in the Sarbanes-Oxley Act of 2002 (also referred to as SOX). For multinational organizations, because of globalization and the rapid development of international communications through the Internet, corporate activities related to environmental degradation, child labor, or other social issues in a developing country have been able to impact profits significantly and quickly in the home country. In addition, the risks associated with Information Technology (IT) installations, mergers, human resource policies, and other daily organizational activities have escalated.

CONTENTS

EXECUTIVE SUMMARY

Risk is an inescapable element of competing in a market economy. Organizations must be able to evaluate many types of risk — political, social, environmental, technological, economic, competitive, and financial — and incorporate the results into decisions regarding investments and operations, as well as into the systems used to monitor and evaluate the effectiveness of the actions taken.

This guideline provides a *Risk Management Payoff Model* that includes a selection of performance measures to properly identify, measure, manage, and report risks. The model demonstrates that improved risk measurement and management not only helps the organization prevent loss, achieve performance and profitability targets, and increase shareholder value, but also produces organization-wide benefits, such as allocation of resources to the risks that really matter, enhanced working conditions, and sustained or improved corporate reputation.

Today, organizations must learn to manage these increased risks. In the publication entitled *Enterprise Risk Management — Integrated Framework*, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) described the underlying principles of risk management and its components. However, boards of directors and their audit committees, senior corporate managers, senior financial managers, auditors, and external stakeholders often need more detailed guidance with respect to the measurement and management of organizational risk.

In addition to the COSO framework and the newly effected regulatory requirements for internal control (see Appendix), this guideline provides a *Risk Management Payoff Model* that includes a selection of performance measures to properly identify, measure, manage, and report risks. The model demonstrates that improved risk measurement and management produces organization-wide benefits, such as enhanced working conditions, allocation of resources to the risks that really matter, and sustained or improved corporate reputation. These consequences help the organization prevent loss, achieve performance and profitability targets, and increase shareholder value. Measuring a broader set of risks more effectively is necessary not only to meet the new regulatory requirements but also, primarily, to improve managerial performance and stakeholder confidence. Risk management involves the identification, evaluation, and mitigation of business risks in order to maximize opportunities and turn risks into sources of competitive advantage.

The ***objectives*** of this guideline are as follows:

- To provide a comprehensive overview of risk management and highlight the role of risk identification and measurement within the risk management process;
- To create a broader framework for risk identification;
- To describe key elements of a measurement model (the Risk Management Payoff Model) for success in dealing with risks strategically and operationally. The model includes the critical *inputs* and *processes* that lead to risk-related *outputs* and ultimately to overall organizational success (*outcomes*). As such, the model helps managers identify and evaluate risks, determine the potential profits of risk management initiatives, and compare different risk responses;
- To outline specific drivers related to these inputs, processes, outputs, and outcomes. By identifying the causal relationships among the drivers, managers can better understand the way in which risk strategies, structures, and systems affect organizational performance;
- To provide specific performance metrics, so that managers can better prepare for, measure, and manage risks; and
- To demonstrate the calculation of return on investment (ROI) for risk management initiatives.

The ***target audience*** of this guideline includes boards of directors, members of audit committees, chief executive officers (CEOs) and chief financial officers (CFOs) with increased responsibilities, senior management teams, and accounting, internal audit, and finance professionals that face the challenges of risk assessment, analysis, and control. The guideline is also aimed at external auditors who must attest to, and report on, internal control over financial reporting.

DRIVERS OF INCREASED RISK AWARENESS

Regulatory Compliance

In recent years, facing more difficult business conditions and the growing expectations of shareholders, some corporate executives — fueled partly by excessive corporate and personal greed — deliberately bent the rules or blatantly reported false financial results for their organizations, causing a series of accounting scandals and corporate failures. These high-profile collapses demonstrated the potential consequences of failing to adopt even the basic principles of risk management as a key component of good corporate governance. In response, the pressure for improved risk assessment has increased throughout the world, taking the form of guidance documents (e.g., the Ontario Securities Commission's proposed policy on effective corporate governance in Canada) and compulsory regulations (e.g., SOX).

Containing some of the most major and radical alterations in securities regulations in the United States since the 1930s, SOX has caused

important changes in public accounting, corporate governance, and internal audit. For many decades, the protection of the investing public focused primarily on financial reporting. It was believed that investors provided with transparent financial results, and the information necessary to understand them, could make fully informed decisions. In 2002, SOX stated that the reporting of financial results was insufficient and required organizations to do more — to analyze and evaluate the quality of the processes and controls used to report these results. In order to harmonize the Canadian regulatory reporting and certification rules with SOX, Canadian Securities Administrators issued a set of proposals entitled *Reporting on Internal Control over Financial Reporting*.

Beyond the Sarbanes-Oxley Act

SOX specifically addresses the evaluation of risks related to financial reporting. However, organizations should look beyond the recent legislation, rather than merely comply with it, and learn to evaluate and monitor other types of risks and their underlying causes. Herein lies the opportunity to develop a business discipline: create formal systems of internal control, detail how these systems will identify, evaluate (measure), and respond to significant risks to the business, monitor these risks, and communicate the results to the appropriate parties. The mismanagement of risk and uncertainty may carry an enormous price. Beyond the traditional financial risk factors, internal and external stakeholders today expect reports on a wider range of issues that can affect future performance, reputation, and financial health.

In general terms, a risk can be described as any event or action that will affect adversely the ability of an organization to achieve its business objectives and execute its strategies successfully. More specifically, risk is the probability that exposure to a hazard will lead to a negative consequence. As such, risks do not arise from internal environments alone. External factors such as technological progress, customer demands, and global forces continuously change business models and increase competitive pressures. Government regulations, deregulation of key industries, and freer trade and investment worldwide create additional uncertainty. Risk is an inescapable element of competition and is integral to the economics of trading, investing, and competing in a market economy.

Thus, organizations need better ways to integrate the consideration of many types of risk — political, social, environmental, technological, economic, competitive, and financial — with the making of management decisions. For example, political instability in a host country, potential product liability, process emissions that are environmentally undesirable, and human resource policies that have social consequences can be important factors in managerial decisions. Organizations must be able to evaluate such risks and incorporate the results into decisions regarding investments and operations, as well as into the systems used to monitor the issues and the effectiveness of the actions taken. This guideline seeks to address these concerns.

Risk Management Pays Off

Many organizations view the effort to comply with SOX as a high-cost, largely administrative exercise. Indeed, significant resources are needed both to comply with regulatory requirements and to manage other risks. Estimates of the costs to comply with the new accounting and auditing regulations range from $400,000 to $750,000 for smaller companies alone. Moreover, these estimates do not include the time executives and other employees must spend dealing with compliance issues. A recent survey conducted by Financial Executives International reveals that a company with more than $5 billion in revenue could expect Section 404 costs of about 0.06 percent of sales, whereas a company garnering less than $100 million could see costs of about 2.55 percent of sales (Katz, 2005). As a result, the number of companies announcing plans to go private has risen steadily since the passage of the Act.

Though there are legitimate concerns about the costs of implementing SOX, organizations should not see the activity as merely an enormous tactical undertaking, producing little more than a list of tasks and corresponding costs. On the contrary, the potential benefits of the new, rigorous examination of risks and controls should be acknowledged. For visionary organizations, the requirements of SOX present a unique opportunity to pursue and implement the best risk management practices. Through the careful and thorough examination process, organizations can become aware of risks that are larger, more varied, and more global than anticipated, assess these risks, prepare appropriate responses, and measure the efficiency and effectiveness of the

risk management initiative. This can result in improved internal control processes, better decision making, increased reliability of information for external users, and enhanced investor confidence.

INCREASED RESPONSIBILITIES IN RISK MANAGEMENT

Because of the new and greater risks in the business environment and the strengthened regulatory requirements for internal controls, the responsibilities of corporate boards, audit committees, and the internal audit function have increased with respect to risk management.

The board of directors has a central role in governance, its primary duty being to promote the long-term interests of the organization and of its shareholders. Epstein and Roy (2002) highlight three critical roles of boards of directors: overseeing strategic direction and risk management, ensuring accountability, and evaluating performance and senior-level staffing. Related to the first is the board's responsibility to review carefully the organizational processes of risk identification, monitoring, and management. Specific reviews of financial objectives, plans, major expenditures, and other significant material transactions should also be included in the board's responsibilities with respect to risk. Although the ultimate risk manager of any organization is the CEO, the board of directors must provide advice and ensure that relevant direction is being given on matters related to risk and internal control.

The audit committee is responsible for examining the performance of the internal control function and the exposure of the organization to a variety of risks. This role has become much more critical. Although there is no regulatory mandate for the implementation of enterprise risk management, the New York Stock Exchange's Corporate Governance Rules require that a listed company's audit committee have a written charter of duties and responsibilities, and that these include discussing policies with respect to risk assessment and risk management. The Rules' commentary notes that, although other mechanisms to assess and manage risk need not be replaced by the audit committee, the audit committee must discuss the company's major financial risk exposures and the management processes in place to monitor and control such exposures. Thus, in order to help focus energies in this area, many organizations are developing and implementing Risk Management Charters that establish the authority, roles, and responsibilities of their audit committees as well as define the scope of the activities of their internal auditors.

Internal auditors now have greater responsibility vis-à-vis the audit committee, the external auditors, and corporate governance in general. Although the responsibility for SOX compliance rests with management, the internal audit function typically has responsibility for the Section 404 review of internal controls over financial reporting and presents documented results to the audit committee and to the external auditors. The external auditors then attest to the adequacy of that review, giving their opinion regarding management's assessment of internal control over financial reporting, and providing their own assessment of internal control over financial reporting. In addition, internal auditors provide independent assurance regarding the risk management process by forming an opinion about the extent to which sound controls have been implemented and maintained to mitigate the significant risks that management has agreed to embrace. Also, internal audit often has primary responsibility for monitoring the ethics and whistle-blower functions to ensure that these comply with company and regulatory requirements.

APPROACHES TO RISK MANAGEMENT

Traditional Approach

Historically, a silo approach has been favored, with different types of risk (e.g., insurance, technology, financial, and environmental risk) being managed independently in separate departments. Usually, there has been little or no coordination of risk management and, often, organizations have been slow to identify new and emerging business risks. Nevertheless, well-managed organizations have always managed risk successfully.

Risk can be viewed as uncertainty, hazard, or opportunity. Traditional risk management has concentrated on the two former views, attempting to reduce the variance between anticipated outcomes and actual results. In contrast, the goal of an organization-wide risk management system is to create, protect, and enhance shareholder value by managing the uncertainties that could affect the achievement

of the organization's objectives either positively (opportunity) or negatively (hazard).

Current Frameworks

Each of the major publications that address the growing importance of comprehensive and integrated risk management suggests ways to assess and manage risks within a generalized framework (e.g., DeLoach, 2000; Shaw, 2003; and McCarthy and Flynn, 2004). The required tasks, which vary in number, generally include establishing a context, identifying risks, analyzing and assessing risks, designing strategies for managing risks, implementing and integrating risk management, measuring, monitoring, and reporting (e.g., AICPA and Canadian Institute of Chartered Accountants, 2000). Typically, these publications do not provide clear guidance as to either the actions that managers should take to identify risks or the specific performance measures that should be implemented for effective risk management.

Among the most prominent works are those published by COSO. In 1992, *Internal Control — Integrated Framework* departed from the traditional internal accounting control model by presenting a broad framework of five interrelated components: control environment, risk assessment, control activities, information and communication, and monitoring. In 2004, *Enterprise Risk Management — Integrated Framework* provided a risk management framework that included key principles and concepts, used a common language, and consisted of eight interrelated components: internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring. Expanding on the internal control framework, this document presented a more extensive treatment of the broader subject of enterprise risk management, including aligning risk appetite and strategy, enhancing risk response decisions, reducing operational surprises and losses, identifying and managing multiple and cross-enterprise risks, seizing opportunities, and improving deployment of capital (COSO, 2004a). Both COSO documents offered clear direction and relevant guidance with respect to the identification and management of risks.

Nevertheless, empirical evidence reveals that companies have difficulties designing and implementing new internal control systems to comply with the regulatory requirements. A recent survey of the US Fortune 500 indicated that less than 30 percent of those organizations had implemented any form of enterprise system to support risk management (Teixeira, 2003). There is an apparent knowledge gap with respect to risk management and in particular, a lack of performance metrics for risk management initiatives. Given the increasing demand for significantly improved risk management, specific risk measurement tools are necessary.

THE PROCESS OF RISK MANAGEMENT

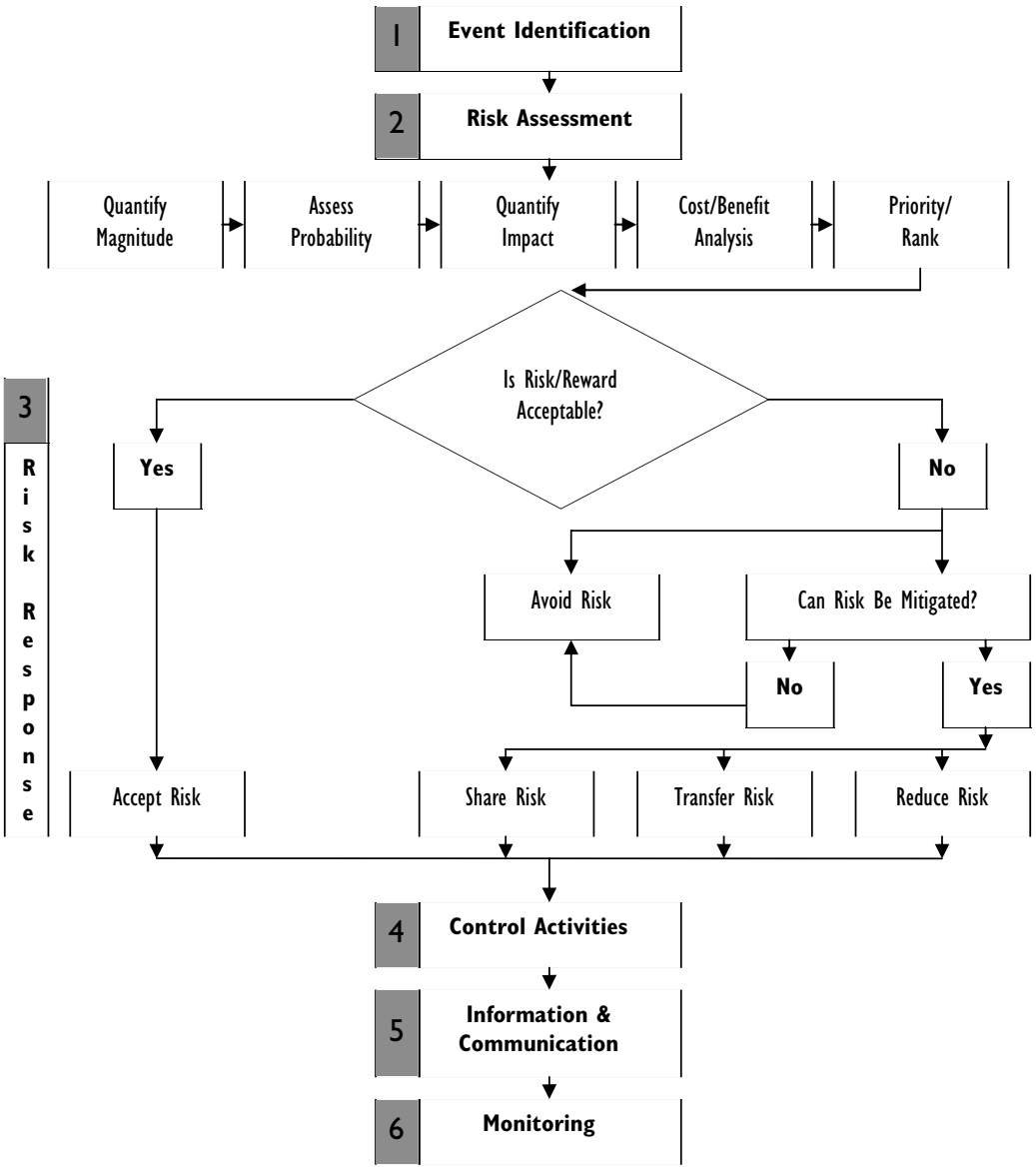
With the speed of change increasing for all organizations, senior managers must deal constantly with a myriad of complex risks that have substantial consequences for their organizations. The goal of risk management is not to eliminate risks, which would also eliminate potential rewards, but to find the right responses to them. Risk management seeks to maximize business opportunities and turn risks into competitive advantage. Effective risk management (see Exhibit 1) involves identifying risks, evaluating potential effects, identifying and analyzing possible solutions, adopting the most appropriate solutions, measuring the results (payoffs) of managing risks, communicating results, and monitoring risk evolution.

Step 1: Event Identification

In today's rapidly changing, complex, and globally oriented businesses, risk is not always apparent. Although, ultimately, the CEO is the organization's chief risk management officer, decision makers at all levels should consider risk identification a critical part of their jobs. Moreover, both managers and employees must learn to spot the warning signs of risks. For example, in the area of human resources, signs of risk could include a change in the demeanor of an employee, a decline in productivity, or a sudden increase in absenteeism. A list of potential risks to the organization could increase the attention paid by managers and employees to the events that might indicate risk occurrence.

There are several ways to classify risks. Building on the COSO framework, Exhibit 2 provides a risk classification scheme that comprises four broad categories of risk — strategic, operational, reporting, and compliance. Strategic risks relate to an organization's choice of strategies to achieve its objectives. Such risks endanger the organization's achievement of high-level goals that support its

Exhibit 1: Risk Management Process

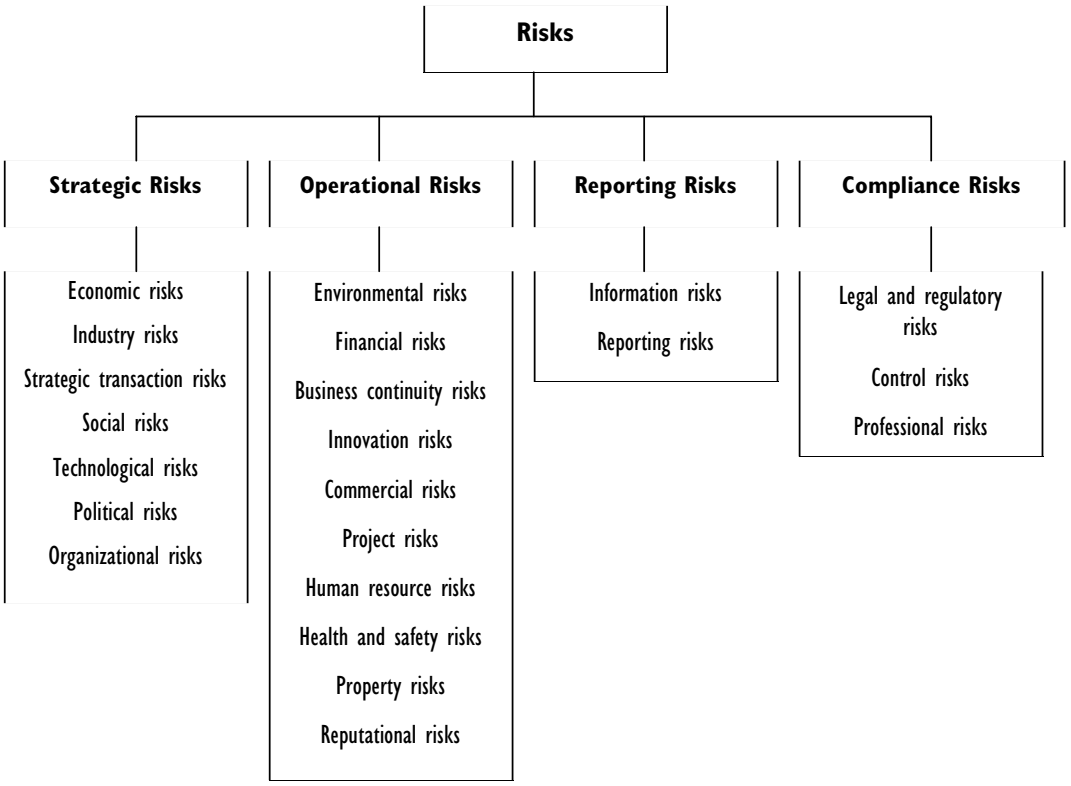


Adapted from Kinney, 2000 and COSO, 2004.

mission, and call into question management's view of the environment. Operational risks relate to the possible loss of organizational assets and include threats from ineffective or inefficient business processes for acquiring, financing, transforming, and marketing goods and services as well as threats to the reputation of the organization. Reporting risks relate to the reliability and accuracy of information systems and to the reliability, timeliness, and completeness of information for internal and external decision making. Finally, compliance risks relate to the communication of laws, regulations, internal codes of behavior, and contract requirements and include the adequacy of information about the failure of management, employees, or trading partners to comply with applicable laws, regulations, contracts, and expected behaviors (Kinney, 2000).

Although controlling compliance risk is recognized as important, regrettably little attention has been focused on improving methods to reduce strategic, operational, and reporting risks. It is true that compliance failures have accounted for the most spectacular organizational losses in the last decade, generating legal costs, tarnishing corporate image, potentially affecting future profitability, and sometimes leading to corporate failure. However, all four categories

Exhibit 2: Risk Classification Scheme



are major sources of organizational risk and deserve an equally high level of managerial attention and relevant response.

The risk classification scheme attempts to define a risk universe and provide a sample listing of organizational risks. To this end, the selected risks included in Exhibit 2, and explained in Exhibits 3, 4, 5, and 6, are representative of the most critical risks faced by organizations today. However, each organization should establish a working list of the risks that are most relevant to its own businesses and business environments.

In each organization, a combination of techniques and supporting tools may be used to identify risks. Approaches include: internal analysis; process flow analysis; creation of event inventories; identification of escalation or threshold triggers; discovery of leading event indicators; loss event data methodologies; facilitated, interactive group workshops and interviews; scenario analysis; and brainstorming sessions.

At Microsoft, the world's leader in the development of software for personal computers, the risk management group spends a great deal of time face-to-face with the business units (Barton et al., 2002). At Telus, one of Canada's leading providers of data, Internet Protocol (IP), voice, and wireless communications services, risk identification involves conducting surveys of various stakeholder groups and asking them to identify possible risks — low, medium, and high — in their areas of responsibility (Telus, 2004).

In the brainstorming approach, participants should be highly visible, represent a broad range of business operations, and have a global perspective of the organization. Some organizations have established a brainstorming team that comprises most of the executive group, including the CEO and the CFO, as well as employees selected for their understanding of different operational areas.

Event identification should ensure that all relevant risks are identified and their sources determined. In this regard, it is important to look beyond silos of risk. For example, when considering the risks of an earthquake, Microsoft managers thought about potential damage to equipment and buildings and, therefore, looked at property insurance. However, management must also take a broader view and consider the elements that are most important to the organization. In the case of an earthquake, the real risk is not that buildings can be damaged but that this can cause an interruption in the

Exhibit 3: Strategic Risks

Risk Type	Definition	Example
Ecomonic Risks	Risks related to macroeconomic policies and economic cycles.	Government's monetary and fiscal policy
Industry Risks	Risks related to competitive positioning, industry profit margins, market structure, and competition laws	Changes in supply and demand, industry concentration, or competitive structure; introduction of new products and services
Strategic Transaction Risks	Risks related to activities undertaken to initiate significant change in strategic direction	Asset reallocation via mergers and acquisitions, spin-offs, alliances, and joint ventures
Social Risks	Risks related to changing demographics and social mores	Child labor; changes in family structures and work/life priorities (human resource issues that could alter demand for products/services or change buying venues)
Technological Risks	Risks related to technological progress and technology-driven disruptive forces	Engineering success/failure; technological obsolescence of product or product assembly (issues that could give a competitor an advantage)
Political Risks	Risks related to changes in government, public policy, and federal oversight, and global risks related to political instability	Management of government relations; terrorist activities
Organizational Risks	Risks related to control systems, business policies, and business culture	Alignment between performance measurement and reward systems

production/business cycle so that the organization cannot do business. The risk identification effort should produce a portfolio of risks, classified as strategic, operational, reporting, and compliance, for the organization as a whole and for every business unit.

Step 2: Risk Assessment

All risks identified as potentially important should be assessed as to their magnitude — the monetary loss or severity of the negative effect if the event should occur. In this regard, it is important to concentrate on the impact of an incident and, especially, on its duration. In addition, the probability of the occurrence of an adverse event of a given magnitude should be determined. The organization can gain a much better understanding of the potential effects of a given risk by calculating both the probability of its occurrence and the expected losses.

Traditional, quantitative techniques for risk measurement and evaluation include: benchmarking; probabilistic models such as value at risk (VAR), cash flow at risk, earnings at risk, development of credit, and operational loss distributions; and non-probabilistic models such as sensitivity models, stress tests, and scenario analyses. In order to quantify the real costs of a risk, its correlation with other risks must be considered as well. Using scenarios may be helpful, particularly in studying the experiences of other organizations.

In addition to the costs that may be incurred if a risk materializes, the benefits that may be provided by an appropriate response to the risk should be assessed. The quantification of both costs and benefits then makes it possible to determine the payoff of a risk management initiative. Traditional risk assessment techniques often focus on those elements that can be

Exhibit 4: Operational Risks

Risk Type	Definition	Example
Environmental Risks	Risks related to the natural environment that could result in damage to buildings, restricted access to raw materials, or loss of human capital	Weather conditions, such as earthquake, fire, or flood; environmental pollution
Financial Risks	Risks related to credit, interest rates, the stock market, currency, and collateral	Foreign exchange rates; strategic equity; asset liquidity; employee stock option program; commodity risks
Business Continuity Risks	Risks related to conditions that could result in work stoppage or adversely affect production, delivery, marketing, supplier and customer management, outsourcing, or compliance with industry and other standards and codes	Reliability within the supply chain; supplier integrity; quality of goods; price of external supply
Innovation Risks	Risks related to the transformation of some aspect of the business in an effort to improve operating performance	Underperformance in new product development and in Research & Development (R&D) investment
Commercial Risks	Risks related to the expected performance of products or services	Quality of engineering, marketing, communication, and sales; product liability in the event of failure
Project Risks	Risks related to the completion of a project	Technical difficulties; commercial obstacles
Human Resource Risks	Risks related to the adequacy and execution of human resource standards, policies, and practices	Ethical/unethical conduct by management and employees; availability of assistance to employees for career planning and personal development; issues that could result in work stoppage, loss of personnel, or monetary or reputational damage
Health and Safety Risks	Risks related to employee health and safety in the workplace	Unsafe equipment or environment; workplace stress; potential for injury from repetitive strain or falls from heights
Property Risks	Risks related to the security of both tangible and intangible assets	Inventory protection against spoilage or theft; intellectual property rights; potential for enforcement action
Reputational Risks	Risks related to the perception of the organization by its stakeholders, the media, and the general public that could impact liquidity, capital, or credit rating	Publicity regarding production methods, business practices, or internal controls

Exhibit 5: Reporting Risks

Risk Type	Definition	Example
Information Risks	Risks related to the quality and accessibility of information	Data accuracy, relevance, reliability, and completeness; security of information; integration of information systems
Reporting Risks	Risks related to the process of capturing, analyzing, and submitting data in a meaningful format to managers and external stakeholders for decision-making purposes	Reliability and completeness of financial information; efficiency of the process for internal decision making and for external reporting

Exhibit 6: Compliance Risks

Risk Type	Definition	Example
Legal and Regulatory Risks	Risks related to meeting legal and regulatory requirements with respect to corporate governance, labor relations, industry standards, the environment, etc.	Employee compliance with the organization's code of conduct and Non-Governmental Organization standards; human rights violations (e.g., child labor)
Control Risks	Risks related to the internal control systems and security policies that could result in system downtime, backlogs, fraud, and the inability to continue business operations	Data integrity; data and system availability; potential for malpractice by employees or outsiders (e.g., theft, deception, forgery, false accounting); potential for operational errors (e.g., clerical, record-keeping, and those resulting from faulty IT systems)
Professional Risks	Risks related to organizational liability and the personal liability of directors and managers	Misrepresentation; defamation; corporate insolvency

quantified easily and fail to address all critical drivers of successful risk management. What is needed is a framework of key factors (antecedents and consequences) that can enable decision makers to assess the impacts of risks in terms not only of the costs but also, and more importantly, of the benefits that successful risk management initiatives may provide. Following is the description of a specific framework that can be used as a tool for risk assessment and risk management. Because of the fundamental nature of risk and its consequences, the Risk Management Payoff Model is equally applicable to for-profit and not-for-profit organizations.

The Risk Management Payoff Model

Business measurement systems are designed to measure and display key success factors for achieving specific objectives. The Risk Management Payoff Model (Exhibit 7) describes the key factors for corporate success in risk management. These include the critical *inputs* and *processes* that are needed for success in risk management *outputs* (e.g., increased regulatory compliance), which then reduce the cost of risk and increase revenues. Finally, the payoff of risk management is determined by its contribution to overall organizational success (*outcomes*) in terms of shareholder value — the ultimate measure of success. This approach helps

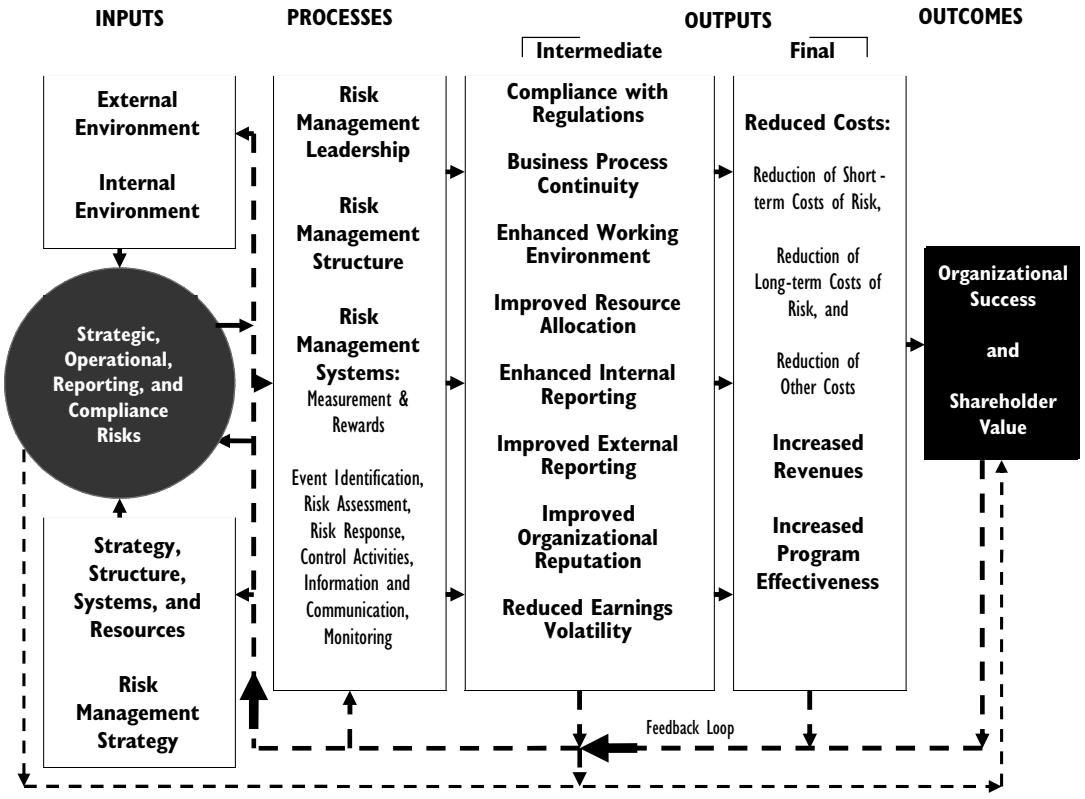
managers understand the critical drivers of reduced long-term risk and related costs as well as increased long-term shareholder value. It also helps managers determine the value of the risk management efforts and improved internal control.

Inputs are the *external environment* in which the organization operates and the *risks* it faces. The organization's ability to develop an appropriate *internal environment* — risk appetite and culture — to respond to external forces, to anticipate risks and allocate resources in its *corporate strategy*, and to develop specific *risk management strategies* to deal with these risks effectively is critical and is reflected in the strategic fit. The better the alignment between the organization's internal strengths and its external opportunities and threats the more effective is the risk management process. Existing organizational and governance *structure* and *systems*, such as incentive pressures, may either support the risk management strategy or inhibit the risk management efforts. Thus, if an organization wants to secure the necessary conditions for effective risk management processes, it must continuously examine its external environment and establish a risk culture and appropriate strategies, structures, and systems in relation to the defined environment. Inputs and processes are the most critical success factors.

Processes involve *risk management leadership, risk management structure*, and *risk management systems*. Committed leadership at the corporate level and focused efforts of the risk management leaders will affect the dedication of employees involved in the event identification, risk assessment, response, and control activities. Together with a carefully designed risk management structure, measurement and reward systems, and IT support systems, this will ensure the achievement of various risk management ***outputs***. These include *intermediate outputs*, such as improved regulatory compliance, business process continuity, or enhanced internal and external reporting, and *final outputs*, such as reduced overall costs and increased revenues. Ultimately, effective risk management should lead to improved overall success and increased shareholder value (***outcomes***).

In Exhibit 8, inputs, processes, outputs (intermediate and final), and outcomes of risk management activities are further articulated as risk management objectives. This is consistent with the COSO framework. The list of risk

Exhibit 7: Risk Management Payoff Model — Antecedents and Consequences of Successful Risk Management



management objectives is not comprehensive; rather, it is an example of the type of objectives that might be selected. Ideally, all objectives should be quantified so that, later, the extent to which the objectives have or have not been achieved can be determined numerically.

After specific risk management objectives have been articulated, the drivers of risk management success (see Exhibit 9) must be determined. In order to identify the specific causes of risks, determine the best way to control them, and analyze the way in which specific risk responses affect overall organizational costs to produce financial benefits, managers need a clear understanding of the most influential drivers of risk management success and their causal relationships.

For example, consider that an organization's risk objective is to prevent unauthorized transactions by employees. On one hand, the organization may invest resources in belief systems (communicating the core values of the company and expected employee behavior) and boundary systems (specifying actions and behaviors that are unacceptable) to prevent the risk from occurring (see Simons, 1999, for more on belief and boundary systems). On the other hand, the organization may increase risk awareness through training and encourage whistle-blowing through appropriate compensation and disciplinary systems, which may result in adequate risk identification, assessment, and response. In both cases, there should be a positive impact on business process continuity, resulting in sustained or increased revenues and decreased costs of risks, or both. Alternatively, if corporate and risk management strategies are aligned, the organization may allocate more resources to risk management initiatives and thereby further the implementation of appropriate boundary and diagnostic control systems, which may lead to the prevention of risks. Higher risk management spending may also increase employee awareness of risk and dedication to event identification, which may lead to timely risk responses. Both the prevention of risks and timely risk responses should enable the organization to sustain business process continuity and thus lead to higher customer satisfaction, sales, and revenues.

Exhibit 9 provides a comprehensive example of risk management drivers and the causal relationships among them. Since the causalities are based on assumptions regarding leading and lagging elements, these hypothesized relationships need to be tested and revised continuously. In practice, there are many more drivers of risk management success than those presented in Exhibit 9. Nevertheless, when examining causal relationships, organizations are likely to articulate fewer drivers so that the illustration is less complex and more easily understandable, thereby allowing managers to focus on the drivers and relationships that are the most critical.

Inputs

The Risk Management Payoff Model is an effective risk assessment framework. In order to use the model to manage risks properly, improve internal control, and create added value, senior managers must first evaluate the inputs — the external elements that will affect the design of the risk management process — with respect to the objectives and drivers of success.

All businesses are exposed to potential hazards. For each organization, the extent of exposure will vary according to the firm's unique characteristics. Managers need to construct a comprehensive list of *risks* faced by the organization in order to ensure that all threats to achieving corporate objectives are assessed adequately, contained to a reasonable degree, and managed economically. Strategic, operational, reporting, and compliance risks, as presented in the risk classification scheme, are thus critical inputs in the Risk Management Payoff Model.

The *external environment* is defined by the industry in which the organization operates; the country-specific political, economic, legal, and social forces; and the location of production and other facilities. These elements affect the risks that the organization faces and should be considered in the design of a risk management system. A Booz Allen Hamilton analysis of 1,200 firms found that the poorest performers destroyed almost seven times more value through strategic missteps related to the business environment (e.g., ineffective reaction to competitive pressures, poor forecasting of customer demand, etc.) than through compliance failures. These findings suggest that, to manage growth, organizations must design robust and integrated strategic planning processes built on a broad understanding of all risks to the business (Kocourek et al., 2004).

Exhibit 8: Risk Management Payoff Model—Setting Risk Management Objectives

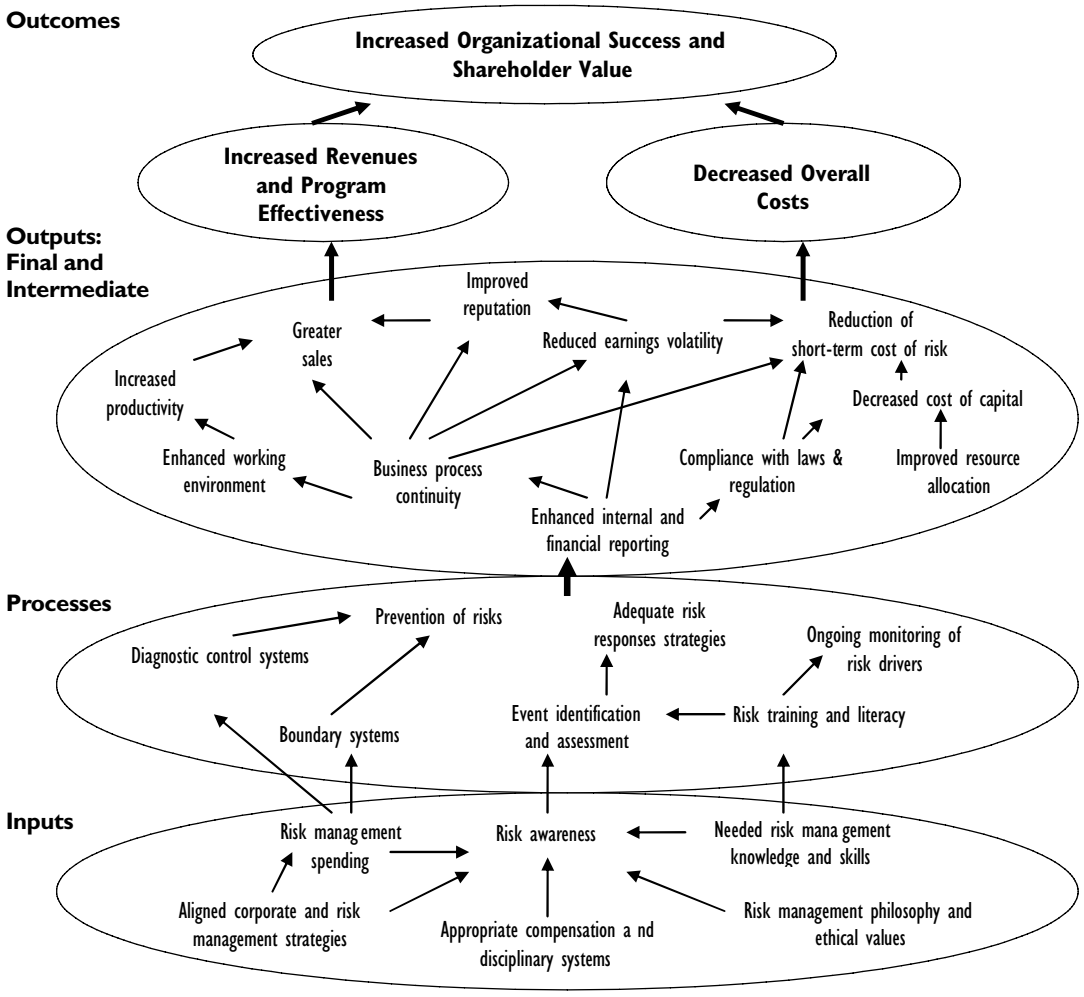
Outcomes	*Increased Long-term Organizational Success and Shareholder Value* *Increased Short-term Organizational Success and Shareholder Value*
Outputs: o **Final**	*Reduced Costs:* Reduction in short-term costs of risk by $1 million *Increased Revenues:* Increase in new-customer sales by $2 million *Increased Program Effectiveness:* 10 percent increase in customer satisfaction
o **Intermediate**	*Regulatory Compliance:* Full compliance with strategically relevant regulations *Business Process Continuity:* Zero unplanned process interruptions *Enhanced Working Environment:* 10 percent increase in labor productivity *Improved Resource Allocation:* Focus on compliance risks *Enhanced Internal Reporting:* Reliable, accurate, and on-time information *Improved External Reporting:* Reliable financial and other reports for external use *Organizational Reputation:* Sustained or enhanced corporate reputation *Reduced Earnings Volatility:* Reduction in earnings distribution *Reduced Cost of Capital:* Reduction in cost of capital by 0.2 percentage points
Processes	*Risk Management Leadership:* Full commitment and focus *Risk Management Structure:* Full integration into business unit structure *Risk Management Systems:* 1. Measurement & Rewards: Optimal balance between belief systems, boundary systems, diagnostic control systems, interactive control systems, and traditional control systems 2. Risk Management Process: Event Identification: Enhanced risk identification techniques Risk Assessment: Increased quantification of risks Risk Response: Adequate risk response strategies Control Activities: Ongoing control of risk responses Information & Communication: High risk awareness throughout the organization Monitoring: Ongoing monitoring activities
Inputs	*Risks:* Development of a list of potential risks *External Environment:* Ongoing monitoring of external environment *Internal Environment:* Appropriate risk management philosophy, integrity, and ethical values *Corporate Strategy:* Strategic fit between the internal potential and external opportunities *Organizational Structure:* Appropriate organizational architecture and governance structure *Organizational Systems:* Suitable training and incentive systems, IT support systems *Organizational Resources:* Adequate capital and people *Risk Management Strategy:* Risk objectives coherent and aligned with the corporate strategy

The *internal environment* is the tone of the organization as revealed in its risk management philosophy, integrity, and ethical values. It is essential that all employees know how their actions affect one another and contribute to achievement of the organization's risk objectives. In addition, developing and maintaining the right corporate culture is extremely important, since employees tend to copy the behavior of their superiors. For example, if employees see dishonesty and corruption at high levels, they often believe that this is acceptable. Some companies with demonstrable risk management processes collapsed (e.g., Enron) partly because they failed to take issues of culture and integrity into account, and procedural controls masked the existence of fraud. The way the business and its controls interact with people and, in particular, the way the organization communicates its attitude toward transgressions are elements of the internal environment that should not be ignored.

Corporate strategy includes both the organization's goals (corporate strategic objectives) in terms of its markets, products, and technologies and the plan for achieving these objectives. An organization expanding its operations to new markets, developing new products, targeting new market segments, or adopting new production technology may face new, more numerous, and more complex risks, which will affect the design of the risk management process.

Another important determinant of the design of the risk management process is the *organizational structure*. This includes the number and geographical location of business units and

Exhibit 9: Risk Management Payoff Model — Drivers of Risk Management Success and Causal Relationships



departments, lines of authority and responsibility, and lines of reporting. An organization with a large number of strategic business units having a high degree of autonomy and spread across a wide geographical area will have a different risk management process than an organization with a simple, centralized organizational structure. It should be noted that organizational structures differ greatly in the handling of risk information and in the associated control mechanisms.

Organizational systems also shape the risk management process and include such elements as control systems, IT support systems, and compensation and disciplinary systems. Belief systems — communicated through mission statements, credos, and statements of values — may create a culture that rewards integrity and clarifies the types of choices that should be made in the face of temptation (Simons, 1999). IT support systems such as software tools may either limit the risk management process or enable the organization to quantify its risks more accurately and prepare alternative scenario analyses. Incentive systems may be aligned with the risk management philosophy, organizational view of integrity, and corporate ethical values or lead to dysfunctional employee behavior. An example of the latter is the case of Bankers Trust Company, a traditional commercial bank whose incentive system rewarded bankers and traders for creating and pushing new products as fast as they could. As a consequence of this incentive pressure, Bankers Trust was sued in 1995 by several clients for misrepresenting the risks associated with new financial products. This resulted in millions of dollars of fines, customer reimbursement costs, and the dismissal of top executives (Simons, 1999).

Organizational resources that are of vital importance to effective risk management include both the financial and the human resources needed for risk prevention, event identification, assessment, response, control, communication, and monitoring. In light of the challenges of complying with Section 404, many public companies are now facing the problem of unqualified or inadequate finance staffs. For example, AXA, an international insurance giant, was found to have insufficient personnel in the corporate accounting department and Advanced Materials Group Inc. was found to be operating with no full-time CFO and a lack of staff expertise (Nyberg, 2004).

Risk management strategy — what the organization aspires to achieve in terms of its risk exposure and risk management — must be consistent with corporate strategy, structure, and systems. Objective setting is an integral part of this input and involves articulating specific operational, reporting, and compliance risk objectives. Risk management strategy must specify the organization's risk appetite (risk tolerance), which may vary with different categories of risk. For example, an organization may have a low risk appetite relative to all compliance objectives but a high risk tolerance for operational objectives that include innovation and commercial risks. Organization-level risk objectives must be integrated with more specific risk objectives for strategic business units and business functions (e.g., IT, human resources, health and safety, production and engineering, etc.).

Processes

After senior managers have evaluated the inputs that affect successful risk management activities, they must plan, develop, and execute risk management processes. Careful attention to both inputs and processes with respect to objectives and success drivers will determine the risk management consequences: outputs and outcomes.

The new regulatory demands on risk management processes and internal controls require a significant shift in thinking and *leadership*. Organizational leadership at all levels — that of the board, senior management, and the risk management group — must be committed to risk management and provide a role model for employees in terms of ethical values and behavior. In addition to regulatory compliance, the leadership focus should be on seizing the opportunities emanating from internal or external sources and gaining competitive advantage. The example of Citigroup, the world's largest bank and a pioneer in international finance, provides a warning. Japanese regulators required the bank to close its private banking unit in Japan for, among other things, failing to guard against money laundering. Senior executives knew that their actions were violating the rules and a number of employees were fired, including three prominent senior executives (O'Brien and Thomas, 2004).

Risk management *structure* provides the framework to plan, execute, control, and monitor risk management activities. Transparency in the assignment of roles and responsibilities to the risk management function enables improved accountability and awareness and, ultimately, improved management and control. A risk

management committee may include the CEO, the CFO, a corporate risk manager, the treasurer, the manager of corporate audit, a compliance manager, and divisional managers. In addition to recommending policy and process, this committee would be responsible for formal reporting to the audit committee of the board of directors on risk management performance. The internal audit function must be structured in such a manner that organizational objectivity is achieved and access to top management and the audit committee is unrestricted.

Many organizations recognize that improved decision making generally results from a well-structured framework for risk and assurance. At United Grain Growers, a Canadian grain handler and distributor of crop inputs, the risk management committee is responsible for assembling comprehensive information on performance in relation to the full range of risk exposures; the previous practice had been limited to reports of adverse experiences with insured risks, treasury, and derivatives trading (Barton et al., 2002). Without an appropriate risk management structure, organizations can easily miss new or changed risks and be unable to exploit opportunities.

Risk management *systems* encompass specific controls aimed at preventing the occurrence of risks. These include belief systems to expound the core values of the business, boundary systems to identify specific actions and behaviors that are unacceptable, diagnostic control systems to monitor critical performance variables, interactive control systems to stimulate learning, and traditional internal control systems (Simons, 1999). Risk management systems may also include compensation and disciplinary systems, specific policies relating to risk training, and human resource standards for hiring the most qualified individuals, with emphasis on educational background, prior work experience, past accomplishments, and evidence of integrity and ethical behavior (COSO, 2004a). Finally, risk management systems incorporate six components of the COSO framework: *event identification, risk assessment, risk response, control activities, information & communication,* and *monitoring*. Organizations must develop appropriate activities for each of these six components.

There must be consistency in the risk management system throughout the organization. For example, every business unit should use the same definition of risk and control, adopt the same criteria for evaluation, follow a standard process for defining what is material or significant, and test to the same extent.

Outputs

Managing risk effectively can result in several beneficial outputs, including compliance with laws and regulations, secured business process continuity, enhanced working environments, better allocation of resources, improved internal reporting and external disclosure, an increase in organizational reputation, reduced cost of capital, and a reduction in earnings volatility. These benefits are all considered to be intermediate outputs because they lead, in turn, to the final outputs of reduced overall costs and increased revenues.

Compliance with laws and regulations includes the adequate design and operation of internal control as well as adherence to other legal guidelines, such as health and safety regulations, anti-competitive practices, commercial and professional indemnity rules, intellectual property regulations, employment practices regulations, and the like. By identifying, assessing, and properly responding to the risks related to laws and regulations, organizations can prevent the tremendous loss of organizational resources and avoid the unnecessary costs of prosecution and penalties.

Business process continuity is reflected in on-time deliveries of products and services, zero unplanned interruptions in the functioning of information systems, zero unplanned production downtime, and generally smooth execution of the business process. This continuity is best achieved through a carefully elaborated risk management framework supported by a disaster recovery plan that covers critical risks, users, systems, and procedures, and is tested and updated to reflect changing conditions at least annually. Maintaining business process continuity is essential to profitability.

Evidence of an *enhanced working environment* can be seen in reduced absenteeism and turnover and in increased productivity and creativity among employees. According to *Health and Safety Executive*, 40.2 million working days were lost in the United Kingdom in 2001-2002 due to work-related illness and injury, representing billions of pounds in lost revenues. Thus, the

ability to identify and manage workplace risks alone can result directly in an increase in productivity and profitability (Cottell, 2003).

Channeling appropriate resources to the most significant risks is more cost-effective and efficient overall. This *improved allocation of resources* is an important result of effective risk identification and measurement and contributes directly to the bottom line.

Based on effective risk management processes, *enhanced internal reporting* of risk and control information can lead to improved decision making with respect to taking on risks knowingly, a more effective balance between risk and reward, and better responsiveness to internal and external activities and change. Improved internal communication and knowledge sharing can increase understanding of the main risks to the business and the effective strategies put in place to address these issues. Reliability, relevance, and timeliness of information will also improve internal reporting of other information, such as financial or operating information, so that heads of business units and senior managers can make better business decisions.

Organizations are required to provide quality information to external stakeholders, and to ensure honest, balanced, and complete external reporting. With a proper risk management framework, an organization can produce reliable *external reporting* that will affect the organization's reputation and shareholder value in a positive way.

Improved organizational reputation is one of the most important outputs of successful risk management activities and the loss of reputation is one of the most significant risks that organizations face today. A recent survey of over 100 CEOs of major European corporations ranked reputational risk as the second biggest threat to business, after business interruption. The same survey also ranked the effective management of reputational risk as the most important opportunity for increasing shareholder value (Blunden and Allen, 2003). A change in reputation impacts not only the immediate earnings of the organization but also several years of future earnings. Damage to an organization's reputation can be accompanied by direct, short-term losses, such as regulatory fines, that affect the profit and loss statement almost immediately. However, most organizations consider the indirect, future loss from public disclosure to be far more significant, as well as more costly.

Organizations can be proactive by building up reputational capital. For example, JP Morgan Chase, a New York-based leader in investment banking and asset management, released a free publication of its value-at-risk methodology that led to the broad adoption of this model in the financial markets and enabled the organization to establish a reputation for cutting-edge risk management (Blunden and Allen, 2003).

Reduction of earnings volatility can be an output of integrated risk management. By bundling the management of various risks into one framework, organizations can not only eliminate the costs of operating multiple programs but also offset a negative experience relative to one risk with a favorable experience relative to another. This can reduce the volatility of earnings, which, in turn, can not only reduce share price volatility but also increase the average share price over time.

Reduced cost of capital is a benefit that for-profit organizations can expect from an integrated risk-financing program. With integrated risk management, an organization can increase its leverage capacity by transferring part of a previously retained risk to a third party. The higher debt levels, carrying a lower cost than equity and forming a greater proportion of total financing costs, reduce the overall cost of capital to the organization. With respect to not-for-profit organizations, the corresponding benefit is the *reduced cost of funds acquisition*.

The intermediate outputs described above result in improvements in two final outputs: notably reduced costs and increased revenues at the organizational level.

Reduced costs include reductions in the short- and long-term costs of risk and in overall costs. The *short-term costs of risk* include the costs of prosecution and penalties. Typically, the reduction of costs in this area is a direct consequence of increased compliance with legislation. For example, implementation of health and safety standards in the workplace prevents work-related injury, illness, and death. The *long-term costs of risk* are reduced as a result of the portfolio effect, which should be of particular interest to all organizations. For example, discounts on the cost of insurance can be given for a wide range of risk management measures, including enhanced security, improved safety equipment, and new safety policies for staff. By bundling risks into a portfolio rather than managing them separately, United Grain Growers was able to use the very low loss ratios on some lines of insurance to offset less favorable loss ratios

on other lines, and integrate insured business risks with non-insurable risks (e.g., grain-handling volume). As a result, the long-term cost of risk was reduced significantly (Barton et al., 2002). *Overall cost reductions* occur when unforeseen events are reduced in number, the associated costs being avoided, and when foreseen risks are planned and well-controlled, the associated costs being reduced.

Increased revenues, in the case of for-profit organizations, and *increased program effectiveness*, in the case of not-for-profit organizations, result from several intermediate outputs. Compliance with regulations has a positive affect on business process continuity, which can increase customer satisfaction and loyalty and lead to higher revenues. An enhanced working environment increases employee satisfaction, motivation, and productivity and can lead to increased sales. Enhanced internal reporting supports better decision making and, together with improved external reporting, can increase organizational reputation, impact stakeholder perceptions and customer satisfaction, and lead to increased revenues.

Outcomes

For the risk management initiatives to be of value, the outputs must pay off eventually in the outcomes of *increased organizational success* and *improved shareholder value*. In other words, organizations can increase corporate success and shareholder value by using integrated risk management to reduce costs, increase revenues, and enhance program effectiveness.

Metrics

In order for senior managers to monitor the drivers and causal relationships in the Risk Management Payoff Model, appropriate measures must be developed that are consistent with, and supportive of, the objectives and drivers of success. The same metrics are not appropriate for every organization. Exhibits 10, 11, 12, 13, and 14 present a selection of possibilities rather than a comprehensive set of measures for effective risk management and internal control. Managers must select or adapt a few metrics that most closely fit the corporate and risk management strategy of their respective organizations.

It is important to focus on the key indicators, rather than introduce indicators for everything that can be measured, and to choose a manageable number of performance measures. In this way, decision makers will be able to focus on the critical elements of organizational success rather than try to cope with every aspect of the risk management process. However, with respect to the metrics for risks (Exhibit 10), organizations should have measures in place for all subcategories of strategic, operational, reporting, and compliance risks that the organization faces.

Managers can encounter various difficulties when applying risk management performance measures. For some metrics, particularly with regard to intermediate and final outputs, existing data may be insufficient. For drivers such as enhanced working environment or increased organizational reputation, managers must establish baseline indicators with initial measurements in order to demonstrate improvement. In order to compile a satisfactory profile of some risks, it may be desirable to gather data going back as far as 15 years. Finally, business risks that are not easily measurable are difficult to quantify at all. When sufficient credible data for a quantitative assessment are not practically available or when the risk does not lend itself to quantification, qualitative techniques must be used for risk evaluation. For example, with respect to technology and regulatory risks, the only measurement that can be made is a subjective ranking based on dollar effects or severity of impact; in such cases, it is common to use a scale from 1 (highly critical) to 3 (least important) with 2 indicating moderate importance.

The results of risk assessment can be projected on a risk map. Individual risks are prioritized on the map according to level of importance (significance), probability (frequency), and potential costs and benefits. In constructing a risk map, managers should consider a plan of three years or longer.

The selection of appropriate performance measures should enable managers to monitor on an ongoing basis the risks to which the organization is exposed, the level of organizational preparedness for coping with risks, and the quality of the organization's risk management process in terms of outputs and financial consequences.

Calculating the Payoff

The implementation of SOX requirements, particularly those related to Section 404, presents organizations with many challenges,

Exhibit 10: Risk Management Payoff Model: Examples of Metrics for Inputs

Inputs	Performance Measures
Risks	o Increase in number of customer complaints about service o Percentage of jobs filled with newcomers o Rate of expansion of operations relative to increase in organizational capacity to invest in more people and technology o Percentage of business based on new products and services generated by creative, risk-taking employees o Increase in frequency of failed deals, new products, or new services
External Environment	o Potential changes in laws and regulations o Political and cultural climate o Availability and cost of labor, materials, and capital o Changing customer tastes and preferences Changes in competitive position of the organization
Internal Environment	o Percentage of employees familiar with the organization's risk management philosophy and risk appetite o Percentage of employees familiar with the organization's risk management strategic objectives o Percentage of employees familiar with the corporate ethical values
Corporate Strategy	o Number of risk management projects approved in the strategic plan o Type of risk management projects (strategic, operational, reporting, and compliance) approved in the strategic plan o Percentage of aggressive stretch goals that are set from the top down with little or no input by subordinates
Organizational Structure	o Level of risk management empowerment experienced by business units and functional managers o Clarity in delegation of risk roles and responsibilities
Organizational Systems	o Likelihood that employees are misconstruing the intentions of senior managers o Likelihood that employees are taking on unacceptable levels of risk for personal gain o Percentage of total compensation represented by performance-variable pay o Percentage of employees ranked for purposes of comparison o Dollars invested in risk-related IT support systems o Percentage of hardware, databases, communications systems, and applications systems that are standardized o Number of IT applications that are not fully integrated with the overall IT system o Percentage of systems developed/maintained outside the organization

(*continued*)

Exhibit 10: Risk Management Payoff Model: Examples of Metrics for Inputs (*cont'd*)

Organizational Resources	o Rate of growth in risk management spending relative to rate of growth in direct total spending o Dollars available for risk management infrastructure investment o Size of systems security budget relative to total risk management budget o Dollars available for employee risk management training and development o Level of employee risk management literacy o Percentage of finance and accounting staff with adequate qualifications
Risk Management Strategy	o Number and scope of risks covered by risk management strategy o Level of integration planned in managing strategic, operational, reporting, and compliance risks o Anticipated increase in corporate reputation due to risk management o Anticipated level of business process continuity due to risk management o Planned reduction in annual total cost of risk o Planned costs, benefits, and profitability of risk management projects

complexities, and new costs. However, with an approach to risk assessment and management that goes beyond the evaluation of internal control over financial reporting, organizations can realize benefits far wider than enhanced investor confidence in financial reporting.

The Risk Management Payoff Model presented in this guideline provides organizations with a framework for the identification and assessment of various risks. Using the metrics selected in the model, managers can also determine the economic payoff of risk management activities. Exhibit 15 illustrates the calculation of ROI for a risk management initiative.

Step 3: Risk Response

In responding to risk, it is important for the organization to consider both the type and scale of risk that it should embrace and the extent to which stakeholders can be expected to accept the commercial consequences, if the risk materializes. Using the quantification process outlined in the Risk Management Payoff Model, the organization can determine the most appropriate response to a given risk and assess the effectiveness of the risk management processes and controls already in place. If these are found to be insufficient or excessive, and thus not cost-effective, the organization can use the knowledge it gains from the Risk Management Payoff Model to reallocate capital or resources.

In general, risk responses include:

- Acceptance (no action taken to affect risk likelihood or impact). Usually, organizations accept risks because they can withstand the impact, they have transferred the risk, or they have reduced the risk to a tolerable level. It is the CEO's responsibility to clarify with the board of directors both the categories of risk and the extent of exposure that are considered acceptable for the organization;
- Sharing (risk likelihood or impact reduced by transferring or otherwise sharing a portion of the risk);
- Transfer (risk passed to an independent, financially capable third party at a reasonable economic cost under a legally enforceable arrangement). For many years, buying insurance was seen as the only risk management tool that organizations could employ. Today, although insurance can help to provide financial security against unforeseeable events, other forms of risk management are essential to help guard against foreseeable risks that essentially remain within the control of the organization.

Exhibit 11: Risk Management Payoff Model: Examples of Metrics for Processes

Processes	Performance Measures
Leadership	o Percentage of senior executives' time dedicated to risk management o Percentage of annual budget allocated to risk management initiatives o Percentage of CEO's and CFO's bonuses linked to decrease in overall cost of risk o Percentage of senior managers literate in risk management
Structure	o Clearly defined and transparent risk management roles and responsibilities o Degree of board's independence from management o Level of experience and expertise of board members o Ratio of risk management support staff to total number of employees o Number of risk management professionals per employee
Systems: *Measurement & Rewards*	o Percentage of employees compensated according to risk management effectiveness o Percentage of employees' variable pay linked to reduced long-term cost of risk o Percentage of risk management support staff receiving pay-for-performance compensation o Percentage of employees aware of the critical performance variables o Frequency of updates to risk policy and procedures o Frequency of government regulations compliance checks
Event Identification	o Percentage of employees involved in the risk identification processes o Number of different risk identification techniques applied o Number of risk identification initiatives using both future- and past-oriented techniques o Number of tests of risk occurrence applied o Percentage of uncertainties identified as risks o Percentage of risks identified that require regulatory compliance o Percentage of risks identified that require competitive repositioning
Risk Assessment	o Percentage of risks assessed with quantitative techniques o Percentage of risk rankings validated by specialists' opinions o Percentage of risks assessed with respect to cost/benefit o Percentage of risk costs sufficiently defined and broken down
Risk Response	o Percentage of risks avoided with no costs o Percentage of risks reduced, transferred, shared, or accepted o Percentage of risks managed integrally

(*continued*)

Exhibit 11: Risk Management Payoff Model: Examples of Metrics for Processes (*continued*)

Processes	Performance Measures
Control Activities	o Percentage of risk responses controlled by top-level reviews o Percentage of risk responses controlled by direct functional or activity managers o Number of executed periodic threat analyses of extremist groups with respect to current operations o Percentage of key areas (units) under camera surveillance to identify potential fraud or illegal activity
Information & Communication	o Percentage of senior managers and employees that understand the objectives of risk management initiatives o Dollars invested in employee risk awareness o Dollars invested in improving risk management skills and knowledge o Percentage of corporate-level performance measures and rewards linked to risk management effectiveness
Monitoring	o Percentage of risk project evaluations based on Return On Investment (ROI) metrics o Percentage of risk management initiatives monitored on an ongoing basis

Exhibit 12: Risk Management Payoff Model: Examples of Metrics for Intermediate Outputs

Intermediate Outputs	Performance Measures
Compliance with Regulations	o Evaluation of effects of proposed or pending legislation on current operations o Percentage of relevant legal and regulatory risks that have been avoided by complete compliance with laws and regulations o Percentage of relevant legal and regulatory risks that have been reduced by partial compliance with laws and regulations
Business Process Continuity	o Percentage of information system downtime that was unplanned o Amount of time saved, previously earmarked for disaster recovery/business continuity efforts o Percentage reduction in operating cycle time o Percentage reduction in ordering, invoicing, tracking, and payment o Average time required to fill and process a customer order o Percentage increase in number of customer orders processed

Exhibit 12: Risk Management Payoff Model: Examples of Metrics for Intermediate Outputs (*continued*)

Intermediate Outputs	Performance Measures
Business Process Continuity (*cont'd*)	o Timeliness in order deliveries o Percentage reduction in customer grievances o Dollars saved based on time saved o Percentage increase in capacity utilization o Change in fixed costs per unit of capacity o Percentage of processes improved
Enhanced Working Environment	o Dollars saved due to improved health and safety conditions o Dollars saved due to decrease in absenteeism o Dollars saved due to lower rate of employee turnover o Dollars saved due to reduction in costs of employee grievances o Dollars saved due to reduction in costs of labor union grievances o Percentage increase in production output per employee o Dollar increase in sales due to productivity improvements o Percentage turnover in risk management support staff
Improved Resource Allocation	o Percentage of risks for which risk management responses were developed as part of an integrated risk-financing program o Financial effects of the integrated risk-financing program
Enhanced Internal Reporting	o Dollars saved due to increased IT security (i.e., reduced IT system downtime, reduced incidence of fraud, etc.) o Dollars saved due to improved information quality (i.e., improved timeliness, accuracy, relevance, etc.) o Time saved due to improved quality of information and internal reports o Change in auditor's evaluation of the quality of internal reports
Improved External Reporting	o Increase in shareholder satisfaction with financial reporting and risk disclosure o Increase in satisfaction of other stakeholders with financial reporting and risk disclosure o Change in auditor's evaluation of the quality of financial reports
Improved Organizational Reputation	o Improved corporate reputation ranking o Frequency of positive media coverage o Improvements in the ratings of corporate brands
Reduced Earnings Volatility	o Percentage reduction in earnings volatility
Reduced Cost of Capital/Funds Acquisition	o Percentage reduction in cost of capital o Percentage reduction in cost of funds acquisition

Exhibit 13: Risk Management Payoff Model: Examples of Metrics for Final Outputs

Final Outputs	Performance Measures
Reduced Costs	o Percentage reduction in costs of prosecution and penalties o Percentage reduction in overall short-term costs of risk o Percentage reduction in overall long-term costs of risk o Percentage reduction in overall operating costs
Increased Revenues	o Increase in sales due to business process continuity o Increase in sales due to improved organizational reputation o Percentage of sales from new customers o Increase in sales from existing customers o Number of new customer partnerships created due to improved regulatory compliance
Increased Program Effectiveness	o Percentage of strategic non-financial goals achieved o Increase in customer satisfaction o Increase in customer loyalty

Exhibit 14: Risk Management Payoff Model: Examples of Metrics for Outcomes

Outcomes	Performance Measures
Long-term Organizational Success/ Shareholder Value	o Percentage change in stock price attributable to risk management initiatives o Percentage of strategic financial goals achieved o Economic Value Added (EVA) o Growth in earnings o Return on Assets (ROA) o Return on Equity (ROE)
Short-term Organizational Success/ Shareholder Value	o Growth in cash flow o Value added per employee o Profitability of risk management projects o Market value of financial instruments relative to contract value

Ways to transfer risk include buying insurance, hedging risk in the capital markets, sharing risk through joint venture investments or strategic alliances, arranging outsourcing that is accompanied by a contractual risk transfer, and indemnifying risk through contractual agreements (DeLoach, 2000);

- Reduction or mitigation (action taken to reduce risk likelihood or impact, or both). Building controls in response to risk is a form of mitigation. The CEO should evaluate the organization's ability to reduce the incidence of risks and the impact on the business; and
- Avoidance (exiting the activities that give rise to risk).

Exhibits 16, 17, 18, and 19 illustrate selected approaches and techniques for the prevention,

Exhibit 15: Risk Management Payoff Model: Calculating ROI for a Risk Management Initiative

CALCULATE THE MONETARY VALUE OF THE BENEFITS OF THE RISK MANAGEMENT INITIATIVE		
Outputs	**Benefits**	**Monetary Value**
Compliance with Regulations	Reduced costs of prosecution and penalties	$.....
Business Process Continuity	Labor hours saved, machine hours saved, reduced cost of grievances, etc. due to increased on-time deliveries	$.....
Enhanced Working Environment	Increase in output (units produced, services offered)	$.....
Improved Resource Allocation	Savings in costs due to efficient capital allocations	$.....
Enhanced Internal and External Reporting	Reduced direct administrative and operating costs, reduced incidence and costs of fraud, etc	$.....
Corporate Reputation	Increased sales from existing and new customers	$.....
Reduced Earnings Volatility	Increase in shareholder value	$.....
Reduced Cost of Capital	Savings in costs of equity financing	$.....
	Total Benefits	$.....

CALCULATE THE TOTAL COSTS OF THE RISK MANAGEMENT INITIATIVE		
Costs		**Value**
Front-end Direct Costs of Risk Initiative	Costs of event identification, assessment, and response (e.g., hardware, software, installation and configuration, training, etc.)	$.....
Disruption Costs Related to Human Factors	Hours lost because of risk training, decline in labor productivity, decline in product and service quality, lost revenues	$.....
Disruption Costs Related to Organizational Factors	Costs of organizational restructuring, technical disruptions, breakdowns in service	$.....
	Total Capital Costs	$.....
Operating Costs of Risk Management Initiative	Costs of control activities, information & communication, and monitoring	$.....
	Total Operating Costs	$.....

CALCULATE THE ROI OF THE RISK MANAGEMENT INITIATIVE
$$ROI = \frac{\text{Total Benefits} - \text{Operating Costs}}{\text{Capital Costs (Investment)}} * 100$$

reduction (mitigation), transfer, and sharing of strategic, operational, reporting and compliance risks. When choosing an approach, an organization will be influenced by its risk appetite, or that of its stakeholders. In addition, the organization should consider the costs of operating particular controls relative to the benefit obtained in managing the risks.

In addition, risk response involves planning and preparing to take action in the event that a disaster occurs. This may include practicing specific responses to hazardous situations or worst-case scenarios.

Step 4: Control

Control policies and procedures are needed to help ensure that the chosen risk responses are carried out properly and in a timely manner. Such activities typically include top-level reviews, direct functional or activity management, and the segregation of duties as well as the use of physical controls, information processing, and performance indicators. Control procedures can be implemented manually or make use of computers or other devices. Because risks change over time, ongoing evaluation is needed of both the risks and the policies and procedures designed to manage and control them.

The Risk Management Payoff Model adds an extra dimension of control. Using the framework outlined above, organizations can determine whether or not the anticipated intermediate and final outputs have been realized and calculate the monetary effects (payoffs) of risk management initiatives. Thus, the model represents a control device for evaluating the efficiency of the risk management process.

Step 5: Information and Communication

Within the organization, effective risk communication is essential. Employees at all levels must understand the definition of risk, the corporate attitude to risk, the organization's exposure to different risks, the consequences of those risks, and the organization's response to them. This information can be disseminated by means of employee manuals, bulletins, and the corporate intranet. In addition, management must provide employees with specific and directed communication that addresses behavioral expectations for individuals and the risk-related responsibilities of personnel. This should include a clear statement of the organization's risk management approach and a clear delegation of authority.

Generally, risk communication should convey the commitment of senior management to the effective management of risk. More specifically, it should convey:

- the importance and relevance of an effective risk management framework;
- the organization's risk-related strategic objectives;
- the organization's risk appetite (risk tolerance); and
- the role and responsibilities of personnel in effecting and supporting the risk management efforts (COSO, 2004a).

Some companies communicate the importance of effective risk management by establishing a link with employee incentives. For example, shareholder value-added (SVA) is applied at JP Morgan Chase (Barton et al., 2002). This metric calculates profit by subtracting a charge for invested capital from cash operating earnings. The more risk taken by a decision maker on the organization's behalf, the higher the capital charge. By introducing SVA, an organization could ensure that all business decisions involve an explicit consideration of risk.

At the board level, risk information must communicate the principal business threats and opportunities, the type of controls that are being implemented, and the relationship between the achievement of strategic and operational objectives and risk performance measures. A top-level risk management report should be provided to both the CEO and the auditor and should ensure that both individuals achieve a clear understanding of the level of risk exposure and the effectiveness of the controls in place.

External stakeholders are interested in the risk-taking policy of the organization, the specific risks to which the organization is exposed, and the way in which those risks are managed. Communication of relevant risk-related information to shareholders, regulators, financial analysts, and other external parties leads to a better understanding of the circumstances and risks the organization faces. In addition, public expectations are growing with respect to reliability and security in financial reporting and in the disclosure of risks. Accordingly, risk-related communication should be meaningful, pertinent, timely, and in conformance with legal and regulatory requirements.

Exhibit 16: Responding to Strategic Risks

Strategic Risks	Approaches and Techniques
Economic Risks	Derivatives (futures, options, and swaps)
Industry Risks	Ensuring compliance with laws and regulations; training employees in compliance culture with respect to their dealings with customers, suppliers, and competitors
Strategic Transaction Risks	Derivatives (futures, options and swaps)
Social Risks	Marketing research; environmental scanning
Technological Risks	Industry analysis; environmental scanning
Political Risks	Lobbying
Organizational Risks	Adopting contemporary management control systems

Step 6: Monitoring

Businesses and circumstances change constantly, and risk management must evolve with them. Therefore, all aspects of the risk management process — risk identification, measurement, response, and control — need to be monitored. Risk-related strategic objectives, success drivers, and performance measures should be updated and elements of risk management modified as necessary. Generally, monitoring can be done in one of two ways: through ongoing activities or by means of stand-alone evaluations. The greater the depth and effectiveness of ongoing monitoring, the less need there is for separate evaluation projects. For example, Johnson & Johnson uses a highly interactive, long-range profit-planning system to assess opportunities and threats on a continuous basis. Under this system, managers constantly revise projections in response to three questions: What has changed? Why? What are we going to do about it? (Simons, 1999).

Given the ongoing changes in corporate governance, organizations also need systems to monitor developments in this area and to identify those aspects of the existing compliance, audit, and risk management programs in which revision is needed. The board of directors should ensure that such a system is implemented. For example, at Telus, the audit committee is responsible for reviewing and monitoring the risk management systems currently in place in order to mitigate the company's exposure. The committee reviews the risk management goals, proposed changes, annual risk assessment flow, benefits, and the risk management matrix and timeline (Telus, 2004).

Another area of risk management that needs to be monitored is the organization's contingency plan for business continuity. If the unexpected were to happen, critical business operations would have to be redeployed quickly, in order to reduce downtime and minimize the impact on productivity and profitability. In 2002, only 28 percent of organizations had a business continuity strategy in place, and this figure was lower in 2001 (McNeill, 2003). Managers need to identify the processes, equipment, and people that are essential for the organization to provide its customers with the products or services they need and, on that basis, construct a contingency plan for maintaining business operations. For the plan to be effective, it must be reviewed and rehearsed on a regular basis. It is advisable that the drills be as real as possible, with computers shut down, for example, or telephones switched off. Unless the plan is tested to this degree, participants, including senior management, may pay little attention to the rehearsal and flaws in the plan may go undetected. In many cases, a proven business continuity plan is essential for insurance coverage and may influence the insurer to retain more of the risk. The process described above can enable an organization to establish a viable plan for business continuity and significantly improve its management of risk.

RISK MANAGEMENT FOR SPECIFIC BUSINESS FUNCTIONS

Although the framework described above proposes measures for managing risks at the organizational level, and for complying with the new regulation on internal control, organizations face similar challenges in measuring and managing risks at the functional level. For example, operations and production

Exhibit 17: Responding to Operational Risks

Operational Risks	Approaches and Techniques
Environmental Risks	Insurance; catastrophe plans and strategies; catastrophe protection products; compliance with environmental laws; certification on ISO 14001 (environmental controls within an organization)
Financial Risks	Regular credit checks on customers; setting terms of trade early in the process, checking invoices, and adopting a follow-up system; factoring and invoice discounting; derivatives (futures, options and swaps)
Business Continuity Risks	Avoiding overreliance on a key supplier; improving supplier management; adequate forecasting of demand; anticipating arrival of new competitors; anticipating a competitor's promotion; coping with variability in production, bottlenecks, and IT systems; determining strategic inventory; establishing efficient internal control systems, rules, and policies; monitoring external risks; certification on ISO 9000:2002 (quality of products and services); outsourcing
Innovation Risks	Derivatives (futures, options and swaps); patent watches; outsourcing
Commercial Risks	Derivatives (futures, options and swaps); ongoing identification of potentially registrable rights; patent watches; securing licenses and permissions; outsourcing
Project Risks	Well-defined project strategy; effective and well-defined project management with identified timelines and milestone markers; clearly defined roles and responsibilities; good understanding of project-specific requirements; effective tax and Value Added Tax (VAT) planning; precise definition and breakdown of costs; good matching of time, cost, and quality; complete and sufficiently detailed timetable; coping with decisions on design; effective monitoring of time and cost; complete operating and maintenance information; outsourcing of specific project activities
Human Resource (HR) Risks	Adequate systems of promotion; regular reviews of staff competencies; effective antidiscrimination policies; transparent and fair compensation schemes; pre-employment health checks to identify existing problems; high-quality supervision and leadership; compliance with employment laws; outsourcing of specific HR activities
Health and Safety Risks	Certification on OHSAS 18001 (health and safety within an organization); compliance with health and safety regulations; development of guidelines for adherence to corporate safety and environmental standards; ongoing health and safety training; regular plant, machinery, and equipment inspections; occupational health programs; ensuring proper fit and suitability of employees' personal protective equipment; employee rotation; routine drills of organizational response to fire and other hazards
Property Risks	Insurance; ongoing identification of potentially registrable rights; adequate inventory and record keeping; securing licenses and permissions; staff training; clearly defined policies and guidelines
Reputational Risks	Investment in branding; investment in socially responsible projects; advertising; political lobbying; communications strategy; maintaining relationships with the media; media training for relevant staff; communication of company policies on ethical conduct and human rights to public security providers; product and service excellence programs

Exhibit 18: Responding to Reporting Risks

Reporting Risks	Approaches and Techniques
Information Risks	Certification on BS 7799 or ISO 17799 (information security standards within an organization); password security and encryptions; careful disposal of information; system design and training; random inspections
Reporting Risks	Certification on BS 7799 or ISO 17799 (information security standards within an organization); password security and encryptions; careful disposal of information

Exhibit 19: Responding to Compliance Risks

Compliance Risks	Approaches and Techniques
Legal and Regulatory Risks	Certification on ISO 14001 (environmental controls within an organization); certification on BS 7799 or ISO 17799 (information security standards within an organization); password security and encryptions; careful disposal of information; system design and training; random inspections; detective controls such as audits
Control Risks	Regular audits and inspections; risk policy, structures, and processes for responding to risk incidents; fraud awareness training; use of passwords and encryption; vetting all new and potential employees and following up on their references; establishing a system that ensures no single employee is in control of a financial transaction from beginning to end; safeguarding company check books and credit cards, maintaining a tight bookkeeping system
Professional Risks	Commercial and professional indemnity; employers' liability coverage; directors' and officers' liability insurance

functions must manage supply chain risks; human resources managers and legal staff need to address personnel risks and health and safety risks; environmental quality managers have to deal with environmental regulation compliance and related risks; and R&D managers must find ways to manage innovation and commercial risks. In addition, many of these business functions have grown in importance recently and experienced increased pressure for accountability with respect to resources used. As a result, specific business functions will find it useful to apply the Risk Management Payoff Model in order to identify, measure, respond to, control, and monitor risks more carefully, as well as calculate the payoffs of risk management initiatives.

INFORMATION RISK

Information is at the heart of risk management, yet is itself a source of risk. Although information technology plays a critical role in many companies today and is expected to extend its influence to virtually all organizations in the near future, most companies do not have a formal process in place to identify potential risks associated with IT, or trace their sources. Information risk can be managed successfully only if IT risk strategies are integrated with the firm's overall business risk strategies. Failure to do so makes it difficult to identify the links between business processes and the business risks that result from the use of IT.

Some of the most worrisome IT risks relate not to the technology itself but to the integrity and security of the information. For example, the information on which management relies for decision making and reporting must be relevant, current, accurate, and representative. In addition, certain information must not fall into the hands of the organization's competitors and thereby become a threat to the business.

The COSO framework specifically addresses the need for controls over IT and information

systems. General controls ensure the continued, proper operation of all application systems and include controls over security management, IT infrastructure and management, and software acquisition, development, and maintenance. Application controls focus directly on the completeness, accuracy, authorization, and validity of data capture and processing. These controls help ensure that data are captured or generated when needed, supporting applications are available, and interface errors are detected quickly (COSO, 2004a). Application controls include balancing activities, digit checks, predefined data listings, data reasonability tests, and logic tests.

It is the responsibility of senior management to clarify what data should be protected, how sensitive this information is, how much protection is needed for different types of data, and how much risk the organization is willing to accept. Armed with this understanding, the IT department can then decide on the best way to provide the necessary security. It is advisable to concentrate responsibility for the security of information in all forms — printed and electronic — under a single management structure.

Once an information security system has been established, organizational culture is a critical factor in ensuring that individual employees pay attention to the information security policies and implement the procedures. It is also important to monitor the system. For example, an overall assurance report can be generated, detailing regular security checks, the exceptions that were found, the effectiveness of escalation procedures in containing incidents, and other relevant information.

RISK ASSESSMENT IN DUE DILIGENCE

Assessing risk is also an important part of the due diligence required with respect to both mergers and acquisitions. Surveys and reports by the media and financial analysts reveal that most mergers fail, and that due diligence is one of the determining factors. Although an acquisition typically involves the much simpler process of fitting a smaller organization into the existing structure of a larger, acquiring organization, the perils of bad risk assessment in due diligence are much the same as those encountered in a merger of equals.

Among the risks associated with mergers and acquisitions are those related to the conversion of existing systems and the initiation of new ones. The integration strategy should be well articulated and indicate the selected systems, processes, and practices that are most relevant to the functioning of the new entity. Targets and milestones must be created, especially for the measurement of synergies. Performance measurement systems must be aligned with the new strategy. Centralization of the IT function may be necessary to ensure compatibility and cohesiveness of data and to avoid adding unnecessary layers of technological complexity to the decision-making process. Specifically, it is critical to prevent deterioration of the key controls that were in place in the two organizations before they merged and to standardize the management of errors. Human resource issues must be handled with speed and clarity; employees of both organizations must be well informed of the severance policies and of the criteria for staff retention and promotion in order to prevent losing employees whose skills are vital to the new firm. Also, the issue of differing compensation programs must be resolved quickly (Epstein, 2004).

Additional risk is associated with the need for integration and conversions to be completed within a short period of time so that the new organization can conduct business seamlessly after the merger/acquisition is formally completed. At the same time, it is vital that legal and regulatory issues be considered carefully. The Risk Management Payoff Model represents a useful tool that can be applied in the context of due diligence to risks encountered both in the merger/acquisition process and in the continuing operations of the new organization.

COMPREHENSIVE RISK MANAGEMENT

Today, the risk management perspective is shifting from a fragmented (departments or business functions managing risks independently), ad hoc (according to need, as perceived by managers), and narrow approach (focused primarily on insurable and financial risks), to one that is integrated, continuous, and broadly focused. Everyone in the organization should view risk management as part of his/her job and risk management efforts should be coordinated through senior-level oversight. The risk management process should be ongoing and all business risks and opportunities considered.

Although the management of many operational risks (e.g., financial) can be assigned to specific departments (e.g., treasury, insurance, audit, health and safety, procurement, etc.) strategic risk management cannot be delegated and remains firmly on the board agenda. It is the responsibility of the CEO to provide the leadership necessary for the active management of strategic risk and he/she must be held accountable for it in his/her annual performance review and evaluation by the board. Strategic risk management should form a significant part of the CEO's job description and be a top priority for both the CEO and the senior management team.

Risk management should become an integral part of strategic and operational decision making throughout the organization. The Risk Management Payoff Model should be applied to all operational and capital investment decisions so that managerial assessment of risk exposure can be part of the decision-making process. Ex ante calculation of the costs and beneficial consequences of alternative scenarios can help managers make the right decisions. For example, if a company plans to expand its operations and build new production facilities in a foreign country, managers must first determine the risks to which the company would be exposed. After carefully evaluating these risks, they must develop alternative risk responses and calculate the costs and benefits associated with each. Similarly, in an organization planning to set up a new incentive system for salespeople, the unintended risks of incentive pressures must be foreseen in various circumstances. In one such scenario, employees feel intense pressure to succeed at all costs, even if their actions overstep ethical bounds, out of fear that failure to meet performance expectations will jeopardize their status and compensation.

Organizations can make risk consideration a part of the decision-making process by:

- articulating the organization's risk management attitude in the mission statement and strategic objectives;
- communicating the risk management philosophy, specifically the link between risk management and strategy; for example, Dupont emphasizes that risk must be managed not in isolation but with a full understanding of what the organization wants to achieve (Barton et al., 2002);
- consistently incorporating risk awareness in the budgets;
- instilling risk awareness in the corporate culture (which may have been focused on other objectives) and enabling employees to become aware of all risks that are faced — both positive and transferable (insurable);
- conducting risk education and training to ensure that employees understand how risks can be identified and managed;
- articulating risk policies and tolerances through the use of analytical tools and risk assessments;
- introducing mechanisms to connect performance evaluation and incentive to risk management initiatives; and
- making risk assessment a required annual exercise within the business units; when participation in these assessments is broad, and the discussion and prioritization of risks thorough, the mindset of managers and employees can be altered so that risk management is viewed no longer as a verification of compliance with rules and regulations but rather as an important part of everyday decision making.

THE ROLE OF SENIOR FINANCIAL MANAGERS

Responding to the pressures of the business environment and stakeholder expectations, organizations are looking beyond regulatory demands to seek significant performance improvements from their risk management activities. This type of risk management, based on a proper risk assessment framework, is much more evolved than the provision of assurance that an organization has complied with corporate and regulatory standards.

The adoption of such organization-wide risk management is a major cultural change for an organization and needs full support from the highest levels of management in order to succeed. Senior financial managers cannot merely delegate the task of implementing risk management initiatives; they must be the champions of the effort. In particular, the personal commitment of the CFO is of vital importance to the rapid, successful introduction of organization-wide risk management. In some organizations, the CFO is a member of the risk management committee. In all cases, risk management must be viewed as an integral component of good, overall business management, rather than a mere adjunct to it.

The Risk Management Payoff Model can help senior financial managers improve internal control over various risks and better manage operational and capital decisions. As a result, reasonable

assurance can be given that both management and the board of directors, in its oversight role, are being made aware in a timely manner of the extent to which the organization is moving toward the achievement of strategic and operational risk objectives.

CONCLUSION

The broad identification and measurement of risk is not easy and most organizations presently lack comprehensive risk evaluation systems. However, over the last few years, increasingly enormous costs have been associated with the failure to identify risks properly, integrate that information into operational and capital investment decisions, and provide adequate control systems and structures to plan for or reduce the risks. Whether these unanticipated costs have been related to financial frauds or ignored external risks, they have impacted corporate profits significantly and sometimes resulted in corporate demise.

The recently increased regulatory and reporting requirements are one response to the critical need for both internal and external decision makers to have better information regarding the risks inherent in business decisions and to focus more explicitly on managing those risks. Some risks are foreseeable and can be planned for or reduced with various tools and techniques. More general business risks must be controlled through systems and structures.

This guideline has provided a Risk Management Payoff Model that carefully articulates the inputs, processes, outputs, and outcomes of organizational activities related to risk management. The model demonstrates that corporate risks can be measured and the results integrated in all management decisions. The extensive set of metrics can be used to evaluate the payoffs of specific risk management initiatives as well as to assess the potential risks involved in decisions related to operations, processes, and capital projects (e.g., changes in performance measurement and reward systems, IT systems, or production facilities) and the costs of those risks to organizational profitability. More rigorous identification and measurement of broad corporate risks can enable senior managers to consider those risks more effectively in their decision making and manage them more successfully for improved corporate performance.

BIBLIOGRAPHY

American Institute of Certified Public Accountants. 2004. *The AICPA Audit Committee Toolkit.* New York: AICPA, Inc.

American Institute of Certified Public Accountants, Special Committee on Assurance Services. 1997. *Report of the Special Committee on Assurance Services.* New York: AICPA, Inc.

American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants. 2000. *Managing Risk in the New Economy.* New York: AICPA, Inc.

Barton, Thomas L., William G. Shenkir, and Paul L. Walker. 2002. *Making Enterprise Risk Management Pay Off*. Upper Saddle River: Financial Times/Prentice Hall PTR.

Blunden, Tony, and Ed Allen. 2003. Reputational Risk. In Jolly, Adam. ed. *Managing Business Risk.* London: Kogan Page.

Braiotta, Louis, Jr. 2004. *The Audit Committee Handbook*. Fourth Edition. Hoboken: John Wiley & Sons, Inc.

Butters, John. 2003. Information at Risk. In Jolly, Adam. ed. *Managing Business Risk*. London: Kogan Page.

Committee of Sponsoring Organizations of the Treadway Commission. 1992. *Internal Control — Integrated Framework.* New York: AICPA, Inc.

Committee of Sponsoring Organizations of the Treadway Commission. 2004a. *Enterprise Risk Management — Integrated Framework: Executive Summary.* New York: AICPA, Inc.

Committee of Sponsoring Organizations of the Treadway Commission. 2004b. *Enterprise Risk Management — Integrated Framework: Application Techniques.* New York: AICPA, Inc.

Cottell, Roger. 2003. Creating a Safe Working Environment. In Jolly, Adam, ed. *Managing Business Risk.* London: Kogan Page.

DeLoach, J. W. 2000. *Organization-wide Risk Management: Strategies for Linking Risk and Opportunity.* London: Financial Times.

Deloitte & Touche LLP. 1997. *Perspectives on Risk for Boards of Directors, Audit Committees, and Management.* Wilton: Deloitte & Touche Tohmatsu International.

Economist Intelligence Unit and Arthur Andersen & Co. 1995. *Managing Business Risks — An Integrated Approach.* New York: The Economist Intelligence Unit.

Epstein, Marc J. 2004. The Drivers of Success in Post-Merger Integration. *Organizational Dynamics*, Vol. 33, No. 2: 174-189.

Epstein, Marc J., and Marie-Josée Roy. 2002. *Measuring and Improving the Performance of Corporate Boards*. Management Accounting Guideline. Hamilton: The Society of Management Accountants of Canada.

Epstein, Marc J., and Robert A. Westbrook. 2001. Linking Actions to Profits in Strategic Decision Making. *MIT Sloan Management Review* (Spring): 39-49.

Green, Scott. 2004. *Manager's Guide to the Sarbanes-Oxley Act: Improving Internal Controls to Prevent Fraud.* Hoboken: John Wiley & Sons, Inc.

Joint Technical Committee OB/7 — Risk Management. 1999. *Joint Australia/New Zealand Standard: Risk Management (revised draft).* Strathfield NSW: Standards Association of Australia.

Katz, David M. 2005. *Smaller Than a Sarbox?* www.CFO.com. March 24.

Kinney, William R. 2000. *Information Quality Assurance and Internal Control for Management Decision Making.* Boston: Irwin McGraw-Hill.

Kocourek, Paul, Jim Newfrock, and Reggie Van Lee. 2004. It's Time to Take Your SOX Off. *Strategy + Business*, Resilience Report, December.

Lander, Guy P. 2004. *What is Sarbanes-Oxley?* New York: McGraw-Hill.

Levene, Lord. 2003. Premium on Managing Business Risk. In Jolly, Adam. ed. *Managing Business Risk. London*: Kogan Page.

Ligos, Melinda. 2004. When Going Public May Not Be Worth It. *The New York Times*, June 3.

McCarthy, Mary P., and Timothy, P. Flynn. 2004. *Risk from the CEO and Board Perspective*. New York: McGraw-Hill.

McNeill, Ian. 2003. Business Continuity. In Jolly, Adam. ed. *Managing Business Risk*. London: Kogan Page.

Moeller, Robert R. 2004. *Sarbanes-Oxley and the New Internal Auditing Rules*. Hoboken: John Wiley & Sons.

Mun, Johnathan. 2004. *Applied Risk Analysis: Moving Beyond Uncertainty in Business.* Hoboken: John Wiley & Sons, Inc.

Nyberg, Alix. 2004. Raising Red Flags. *CFO*, September.

O'Brien, Timothy, and Landon Thomas. 2004. It's Cleanup Time at Citi. *The New York Times*, November 7.

PriceWaterhouseCoopers. 2004. *Sarbanes-Oxley Act: Section 404. Practical Guidance for Management.*

Ramos, Michael. 2004. *How to Comply with Sarbanes-Oxley Section 404: Assessing the Effectiveness of Internal Control.* Hoboken: John Wiley & Sons, Inc.

Ropeik, David, and George Gray. 2002. *Risk: A Practical Guide for Deciding What's Really Safe and What's Really Dangerous in the World Around You*. Boston: Houghton Mifflin Organization.

Shaw, John C. 2003. *Corporate Governance & Risk: A Systems Approach.* Hoboken: John Wiley & Sons, Inc.

Sheridan, Fiona. 2003. Implementing Sarbanes-Oxley Section 404. In Jolly, Adam. ed. *Managing Business Risk*. London: Kogan Page.

Simons, Robert. 1999. How Risky Is Your Company? *Harvard Business Review* (May-June): 85-94.

Teixeira, Tom. 2003. Enterprise Risk Management. In Jolly, Adam. ed. *Managing Business Risk*. London: Kogan Page.

Telus. 2004. *Leading the Way.* Notice of Annual General Meeting, Information Circular.

Tivey, Andrew, and Ellynne Dec. 2003. Quantifying Uncertainty. In Jolly, Adam. ed. *Managing Business Risk*. London: Kogan Page.

Turnbull Report. 1999. *Internal Control, Guidance for Directors on the Combined Code*. London: ICAEW. See www.icaew.co.uk.

APPENDIX: REGULATORY REQUIREMENTS ON ENHANCED INTERNAL CONTROL

The Sarbanes Oxley Act of 2002 — Section 302 and 404 Requirements

The Sarbanes-Oxley Act of 2002 creates new requirements for managers and accounting professionals related to corporate governance, including the responsibilities of directors and officers, the regulation of accounting firms that audit public organizations, corporate reporting, and enforcement. Sections 302 and 404 particularly have created significant new requirements related to internal control and the assessment of risk.

Under Section 302, the chief executive and financial officers of each publicly reporting company are required to certify each periodic (i.e., quarterly and annual) report filed or submitted to the SEC. The chief executive officer and chief financial officer must sign the certification themselves — another executive under a power of attorney cannot sign the certification. Section 302 requires the certification to cover the review of the report, its material accuracy, and fair presentation of financial information, disclosure controls, and internal accounting controls.

The internal control requirements in Section 404 represent among the more important aspects of the act to a corporation and its external auditors. Management always has been responsible for preparing periodic financial reports; external auditors reviewed those financial numbers and certified that they were fairly stated as part of their audit. Under the Sarbanes-Oxley Act, management now is responsible for documenting and testing its internal financial controls in order to prepare a report on their effectiveness. More specifically, management's process for evaluating the effectiveness of the company's internal controls must include:

- Determination of which controls are significant, which should include controls over transactions (routine, non-routine, estimation and judgment), fraud, controls on which other significant controls are dependent on the financial statement close process, and the locations or reporting entities to be included in the evaluation;
- The documentation of controls related to management's assertion, including each of the five COSO definitions of internal control, controls designed to detect or prevent frauds or errors in significant accounts, transactions or disclosures, the financial statement close process, and controls over safeguarding of assets;
- Evaluation of design and most effective combination of manual and IT controls;
- Evaluation of the operating effectiveness by the testing of controls by internal audit or third parties under the direction of management, or a self-assessment process that includes procedures to verify that controls are working effectively. Inquiry alone is not adequate; and
- Determination of which control deficiencies constitute significant deficiencies or material weaknesses (Sheridan, 2003).

A self-assessment alone is not enough without the documentation and testing to back it up. The external auditors also review the supporting materials leading up to the internal financial controls report to assert that the report is an accurate description of that internal control environment. The report should cover key information such as risk control description, specification of those performing the control, types of controls, frequency, evidence, and results of testing from an efficiency point of view.

Federal Sentencing Guidelines

The United States Sentencing Commission announced that on November 1, 2004, stricter Federal Sentencing Guidelines for organizations would be effective. These guidelines define the essential elements of a corporate compliance program. All U.S. companies, regardless whether they are public or private, are required to have compliance plans if they wish to receive the benefit of prosecutorial discretion from a federal prosecutor, or sentencing mitigation from a federal judge. The primary purpose of a compliance program is to avoid these situations altogether by preventing violations of the law from occurring.

The Federal Sentencing Guidelines set forth seven basic criteria, as follows:

1. Establish standards and procedures reasonably capable of reducing the chances of criminal conduct;
2. Appointment of compliance officer(s) to oversee plans;
3. Take due care not to delegate substantial discretionary authority to individuals who the organization knows, or should know, are likely to engage in illegal conduct;

4. Establish steps to effectively communicate the organization's compliance standards and procedures to all employees;
5. Take reasonable steps to ensure compliance through monitoring and auditing;
6. Employ consistent disciplinary mechanisms; and
7. When an offense is detected, take all reasonable steps to prevent future similar offenses, including modifying the compliance plan, when appropriate.

Canadian Regulation

In Canada, on February 4, 2005, the Canadian Securities Administrators released proposed requirements maintaining the harmonization of Canadian regulatory reporting and certification rules with Sarbanes-Oxley. The proposed Multilateral Instrument 52-111, Reporting on Internal Control over Financial Reporting, requires reporting issuers on the Toronto Stock Exchange to adhere to the following:

- Management will be required to issue a report on the effectiveness of internal control over financial reporting; and
- The external auditor will be required to issue an audit report on management's assessment along with its own report.

The earliest that the proposed instrument will be effective is for fiscal years ending on or after June 30, 2007.

This *Management Accounting Guideline* was prepared with the advice and counsel of:

Kent Allingham, MBA, CPA
Senior Manager, Corporate IT Controls
MCI

Barry Baptie, MBA, CMA, FCMA
Board of Directors
VCom Inc.

Dennis C. Daly, CMA
Professor of Accounting
Metropolitan State University

William Langdon, CMA, FCMA
Vice President, Knowledge Management
CMA Canada

Melanie Woodward McGee, MS, CPA, CFE
Manager of Accounting/Joint Venture
Controller
American Airlines/Texas Aero Engine
Services, LLC

John F. Morrow, CPA
Vice President, The New Finance
American Institute of Certified Public
Accountants

Kevin Simpson, MBA, CM&A, CPA
Managing Director
Focus Business Services, LLC

William H. Steeves, B.Sc., CMA, FCMA
Board Director and Business Consultant

Derrick Sturge, MBA, CMA, FCMA, FCA
Firm Director, CFO and Governance Services,
Deloitte & Touche, LLP

Al Wallace
Chief Operational Officer (COO)
WorkCare Inc.

Kenneth W. Witt, CPA
Technical Manager, The New Finance
American Institute of Certified Public
Accountants

For additional copies or for more information on other products available contact:

In the U.S.A.: **American Institute of Certified Public Accountants**
1211 Avenue of the Americas
New York, NY 10036-8775 USA
Tel (888) 777-7077, FAX (800) 362-5066
www.aicpa.org
Visit the AICPA store at www.cpa2biz.com

In Canada and elsewhere: **The Society of Management Accountants of Canada**
Mississauga Executive Centre
One Robert Speck Parkway, Suite 1400
Mississauga, ON L4Z 3M3 Canada
Tel (905) 949-4200
FAX (905) 949-0888
www.cma-canada.org

AICPA Member and
Public Information:
www.aicpa.org

AICPA Online Store:
www.cpa2biz.com

ISO Certified

030001