

Statement on Management Accounting

Implementing Enterprise Risk Management

Institute of Management Accounting

William G. Shenkir, Ph.D., CPA
William Stamps Farish Professor
McIntire School of Commerce
University of Virginia

Paul L. Walker, Ph.D., CPA
Associate Professor
McIntire School of Commerce
University of Virginia

© 2006 Institute of Management Accountants

TABLE OF CONTENTS

		Paragraph
I.	Rationale.....	1
II.	Scope.....	6
III.	Defining Risk and ERM.....	9
IV.	Total Risk Classification.....	12
V.	The Role of the Management Accountant.....	14
VI.	ERM Frameworks: A Global Perspective.....	18
	The Combined Code and Turnbull Guidance.....	19
	King II Report.....	22
	<i>A Risk Management Standard</i> by Federation of European Risk Management Association (FERMA).....	24
	Australian/New Zealand Standard— <i>Risk Management</i>	25
	COSO’s <i>Enterprise Risk Management—Integrated Framework</i>	28
	IMA’s <i>Collaborative Assurance and Risk Design—Management Edition</i> (CARD-ME).....	31
VII.	ERM Foundational Elements.....	33
	Organizational Context.....	34
	The Tone at the Top.....	35
	Risk Management Philosophy and Risk Appetite.....	36
	Integrity and Ethical Values.....	39
	Scope and Infrastructure for ERM.....	41
	Basic Components of ERM Framework.....	42
	Set Strategy and Objectives.....	43
	Identify Risks.....	45
	Assess Risks.....	46
	Treat and Control Risks.....	53
	Communicate and Monitor.....	57
VIII.	Integrating ERM in OnGoing Management Activities.....	59
	Strategic Planning.....	60
	Balanced Scorecard (BSC).....	62
	Budgeting.....	65
	Business Continuity (Crisis Management).....	68
	Corporate Governance.....	71
	The Board and Stock Exchanges.....	74

	Risk Disclosures.....	76
	Proxy Statements.....	77
	Management’s Discussion and Analysis (MD&A).....	78
	10-K Item 1A—Risk Factor Disclosure.....	79
	Other Voluntary Disclosures.....	80
IX.	Transitioning from SOX to ERM.....	82
X.	Conclusion.....	85
	Glossary	
	Bibliography	

TABLE OF EXHIBITS

Following Paragraph

Exhibit 1: Australia/New Zealand Standard—Risk Management Process—Overview.....	26
Exhibit 2: COSO Enterprise Risk Management Framework.....	28
Exhibit 3: COSO Enterprise Risk Components.....	28
Exhibit 4: A Continuous Risk Management Process.....	42
Exhibit 5: Risk Identification Techniques.....	45
Exhibit 6: Risk Quantification and Qualitative Techniques.....	46
Exhibit 7: Subjective Assessment of Risk.....	47
Exhibit 8: Risk Map.....	48
Exhibit 9: Risk Map.....	49
Exhibit 10: Color Coded Risk Map.....	50
Exhibit 11: Functional Risk Assessment Summary.....	51
Exhibit 12: Linking Objectives, Events, Risk Assessment and Risk Response.....	53
Exhibit 13: Balanced Scorecard and Strategic Risk Assessment.....	64
Exhibit 14: Risk/Crisis Acceleration.....	70
Exhibit 15: Hallmarks of Best-Practice ERM.....	86

I. RATIONALE

1. Leadership is about making a difference. If leaders of organizations in the twenty-first century are to make a difference and grow their organizations to greatness, they must have the capability to navigate in a very risky and dangerous world. Thus, understanding and managing risk has become imperative for successful leadership of organizations in today's world.
2. A variety of risks confront organizations today and any one of them could threaten an organization's success and ultimately lead to a decrease in shareholder value. The need for a greater awareness of risk by leaders is driven by much more than just terrorism and al-Qaeda. Forces such as globalization and the geo-political environment in which organizations operate add complexity to business, thereby increasing risks. Technology and the Internet are requiring companies to rethink their business models, core strategies, and target markets. Customers have ever-increasing demands for both product variety and quality, leading to more risks. If customer expectations are not met, market share, and ultimately revenue and profits, can be significantly and quickly impacted. Organizations must also comply with increased regulations in some cases and in other cases deregulation, both of which drive risks. Mergers and restructurings are causing organizations to downsize and undergo changes in management responsibilities creating risks.

3. Another important driver for more attention to risk management is the accounting and reporting deficiencies, such as unjustified revenue recognition and convoluted business transactions as found in special purpose entities and backdating of stock options. More complex financial instruments like derivatives are also part of the reality today requiring greater understanding of the risks embedded in such instruments. Given all of these forces, leaders must have a heightened state of awareness of the necessity for risk management and for a stronger governance structure for their organization.
4. Well-managed organizations have always had some focus on risk management, but typically it has been on an exposure-by-exposure basis through various risk management silos. For example, the treasury function focused on risks emanating from foreign currencies, interest rates, and commodities—so called financial risks. An organization's insurance group focused on hazard risks such as fire and accidents. Operating management looked after various operational risks, and the information technology group was concerned with security and systems risks. The accounting and internal audit function focused on risks caused by inadequate internal controls. The general assumption was that executive management had their eye on the big picture of strategic risks.
5. As organizations grow in complexity and serve global markets, the leadership challenge is to understand fully how the various business units interact and

relate, and, in turn, how the risks cut across the silos. Instead of managing risk in many individual silos, enterprise risk management (ERM) takes an integrated and holistic perspective on risks facing an organization. Risk-centric leadership does not mean that the organization will be risk adverse, but that in taking risks, the leadership does so intentionally rather than unknowingly and strives to identify, assess, and manage risks.

II. SCOPE

6. This document provides an overview of the ERM process and ERM frameworks. ERM frameworks can be adapted to fit the specifics of the organization's culture and can be implemented in large or small organizations, service or manufacturing businesses, and profit or not-for profit entities.
7. The information in this SMA provides management accountants and other interested parties implementing ERM with:
 - a definition of ERM;
 - a classification of various risks;
 - an understanding of the roles and responsibilities of management accountants in ERM projects;
 - an overview of ERM frameworks from several different professional organizations around the world;
 - a discussion of the foundational elements of ERM;

- suggestions of how ERM can enhance on-going management activities;
and
 - ideas for adding value to the Sarbanes-Oxley (SOX) 404 requirement by extending from risks related to financial reporting to ERM.
8. The information in this SMA serves as a point of departure for an organization considering implementation of ERM. However, this document does not claim to provide a comprehensive discussion of ERM. Other sources identified in the bibliography should also be consulted.

III. DEFINING RISK AND ERM

9. Organizations are confronted by events that affect the execution of their strategies and achievement of their objectives. These events can have a negative impact (risks), a positive impact (opportunities), or an event can contain both risk and opportunity. In the publication entitled *Enterprise Risk Management—Integrated Framework: Executive Summary Framework*, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) defined ERM as follows:
- “A process, ongoing and flowing through an entity
 - Effected by people at every level of an organization
 - Applied in strategy setting

- Applied across the enterprise, at every level and unit, and includes taking an entity-level portfolio view of risk
- Designed to identify potential events that, if they occur, will affect the entity and to manage risk within its risk appetite
- Able to provide reasonable assurance to an entity's management and board of directors
- Geared to achievement of objectives in one or more separate but overlapping categories.”

10. Several points to emphasize from this broad definition include:

- risk management should be viewed as a core competency;
- it is part of everyone's job whether at the level of setting the organization's strategy, a unit's objectives, or running the daily operations; and
- it involves alignment of strategies, processes, systems, people, and information technology so that management and the work-force become more attentive to risk.

11. Organizations seek to create value for their stakeholders, and ERM is implemented with that goal in mind. The authors of this SMA have stated in previous publications that the goal of ERM is “to create, protect, and enhance shareholder value by managing the uncertainties that could either negatively or positively influence achievement of the organization's objectives.”

IV. TOTAL RISK CLASSIFICATION

12. Taking the perspective of the total entity, risks may be classified in a variety of risk frameworks. One frequently used framework is as follows:
- “Strategic Risk – examples include risks related to strategy, political, economic, regulatory and global market conditions; also could include reputation risk, leadership risk, brand risk, and changing customer needs.
 - Operational Risks – risks related to the organization’s systems, processes, technology, and people.
 - Financial Risks – includes risks from volatility in foreign currencies, interest rates, and commodities; also could include credit risk, liquidity risk, and market risk.
 - Hazard Risk –risks that are insurable such as natural disasters; various insurable liabilities; impairment of physical assets; terrorism.”¹
13. Traditional risk management generally focused on financial risk and hazard risk. Approaching risk from an enterprise-wide perspective should enable management to identify most of the key risks that confront the organization. However, implementing ERM does not mean that an organization will be able to anticipate every risk that could result in loss of shareholder value. The limitation of ERM is captured in this statement: “There are knowns, known

¹ *Enterprise Risk Management: Pulling it All Together*, 2002: 3.

unknowns, and unknown unknowns.” (Author unknown.) In the ERM process, known risks will be identified and some previously unknown risks will become known. However, even with a robust process some unknown risks will not be identified. The organization must have a business continuity or crisis management plan ready to execute when unknown risks materialize and negatively affect the organization. Alternatively, unknown risks can create unique opportunities—companies must be ready to capitalize on those opportunities.

V. THE ROLE OF THE MANAGEMENT ACCOUNTANT

14. Adopting ERM is a major commitment for an organization. Successful implementation requires champions at the C-level (CEO, CFO, Controller, Chief Audit Executive, Chief Information Officer) of the organization. Some companies have appointed Chief Risk Officers or established executive level risk committees. The ERM initiative gains momentum when strongly supported by the board of directors and its audit committee. Executive management cannot merely begin the process and then go on to other activities. The last thing most organizations need is another mandate imposed from on high and then left to wither and fade away. If ERM implementation is to be successful, it cannot be viewed as “another program from headquarters,” or the “management fad of the month.”

15. It is important for executive management to communicate that they view ERM as an integral component of sound business management. Implementing an integrated and holistic risk management approach across the entire organization will undoubtedly affect the role of some well-ensconced fiefdoms engaged in silo risk management. Risk champions can be influential in getting general acceptance of ERM across the organization. If the risk management silos are not too strong or high initially, ERM probably has a better chance for broad acceptance.
16. The management accountant can make major contributions to moving the organization from silo risk management to an integrated and holistic approach. Some specific activities where the skills and competencies of the finance professional can be useful in ERM implementation include:
- serve as a champion for ERM;
 - support the change from risk management in silos to ERM;
 - help to resolve conflict between supporters of ERM and traditional risk management approaches;
 - educate others in the organization on the ERM process;
 - provide expertise to operational management on the organization's ERM framework and process;
 - serve on cross-functional ERM committees;
 - assist executive management in setting the organization's risk appetite and risk tolerances for individual units;
 - assist in implementing ERM within the finance function;

- provide information to operational management to assist in risk identification;
- perform benchmarking studies for use in risk identification;
- gather best practice information on ERM;
- assist in quantifying impact and likelihood of individual risk on risk maps;
- assist in identifying and estimating costs and benefits of various risk mitigation alternatives;
- coach management in responding to risks;
- design reports to monitor risks;
- develop financial and non-financial metrics to evaluate the effectiveness of risk mitigation (treatment) actions;
- advise management on integrating ERM with the balanced scorecard and budgeting process;
- participate in development of business continuity (crisis management) plans;
- advise on risk disclosures in the SEC Form 10-K and the annual report;
- serve as a champion for strong corporate governance incorporating ERM; and
- coach management on the value of extending SOX 404 compliance to include ERM.

17. Once executive management has decided to embark on implementing ERM, it is in the enlightened self-interest of management accountants to do what they can to keep the project moving. An effective ERM implementation provides a context for management accountants to perform their duties and responsibilities knowing that people at all levels of the organization have a risk

awareness in doing their work and are held accountable for how they manage risks.

VI. ERM FRAMEWORKS: A GLOBAL PERSPECTIVE

18. ERM is a globally accepted and growing field, and as a result, a number of risk frameworks and statements have been published by professional organizations around the world. Some of the publications urge businesses to use these frameworks. Other risk frameworks have a “comply or explain why not” approach. Still other frameworks are legally mandated or implied in their respective country. Some of the documents were written by accounting and auditing organizations such as COSO, while others were written by individuals with a wider range of backgrounds such as insurance, government, safety and engineering. The different backgrounds lead to very different approaches in these risk frameworks. Some lean towards financial reporting and internal control, and others lean towards management, corporate governance, and accountability. Ambitiously, some even try to cover every possible aspect of risk. Still, enterprise risk management frameworks are valuable tools. They usually provide a diagram or approach that includes the steps necessary for ERM implementation in addition to providing guidance and examples. In this section, the following ERM frameworks are briefly discussed:

- The Combined Code and Turnbull Guidance

- King II Report
- *A Risk Management Standard* by European Risk Management Association (FERMA)
- Australian /New Zealand Standard—*Risk Management*
- COSO’s *Enterprise Risk Management—Integrated Framework*
- IMA’s *Collaborative Assurance and Risk Design—Management Edition* (CARD-ME)

The Combined Code and Turnbull Guidance

19. In the United Kingdom, the Financial Reporting Council published in 2003 the *Combined Code on Corporate Governance* (the Code). Although the Code is not specifically labeled as an ERM framework, it does have many similar aspects, and “risk” is mentioned more than a hundred times. The Code states that the role of the board is to provide a framework of effective control so that risk is assessed and managed. The board is also required to review the effectiveness of controls, including all controls over financial, operational, and compliance areas as well as risk management systems.
20. The Financial Reporting Council also published in 2005 *Internal Control – Revised Guidance for Directors on the Combined Code*, which is a revision of the Turnbull report first published in 1999. This guidance assumes a company’s board uses a risk-based approach to internal control. The guidance

suggests that to assess a company's risk and control processes, the following elements must be reviewed:

- risk assessment;
- control environment and control activities;
- information and communication; and
- monitoring.

21. The guidance offers sample questions that could be used to assess the effectiveness of risk and control processes. Related to risk assessment, questions focus on the presence of clear objectives, effective direction on risk assessment, measurable performance targets, identification and assessment of all risks on an ongoing basis, and a clear understanding of acceptable risks.

King II Report

22. *The King Report on Corporate Governance for South Africa* (King II Report) was published in 2002 to promote corporate governance. This report has five sections:

- board and directors;
- risk management;
- internal audit;
- integrated sustainability reporting; and
- accounting and auditing.

The King II Report also includes an appendix on “risk management and internal

controls.”

23. According to this report, the board is responsible for the risk management process and its effectiveness. The board should:
- set risk strategy policies;
 - assess the risk process;
 - assess the risk exposures such as physical and operational risks, human resource risks, technology risks, business continuity and disaster recovery, credit and market risks, and compliance risks;
 - review the risk management process and significant risks facing the company;
 - and
 - be responsible for risk management disclosures.

A Risk Management Standard by Federation of European Risk Management Association (FERMA)

24. A consortium of UK organizations, including the Institute of Risk Management, the Association of Insurance and Risk Managers, and the National Forum for Risk Management in the Public Sector, published *A Risk Management Standard (RMS)* in 2004. The RMS represents best practice and companies can compare themselves against it to determine how well they are doing in the prescribed areas. It is not a lengthy document, but it does provide a risk management process that includes:
- linkage to the organization’s strategic objectives;

- risk assessment, which the RMS breaks down into risk analysis, risk identification, risk description, risk estimation, and risk evaluation;
- risk reporting;
- decision;
- risk treatment;
- residual risk reporting; and
- monitoring.

Australian/New Zealand Standard—*Risk Management*

25. Australia and New Zealand formed a joint technical committee composed of representatives from numerous organizations to publish two documents on risk management in 2004. The committee is diverse and includes groups that focus on computers, customs, insurance, defense, emergency management, safety, securities, and accounting among many others. This diverse background leads to a different approach than that seen in other frameworks. The first document is a standard entitled *Risk Management* (the Standard), which was initially published in 1999, and the second companion document entitled *Risk Management Guidelines* (the Guidance) provides insights on implementing the Standard.
26. The Standard can be applied to any type of organization and to any project or product. It attempts to factor in both the upside and downside of risk. Although the Standard specifies the elements of risk management, it is not intended to enforce uniformity.

The Standard's objective is to provide guidance in several areas, some of which are: a basis for decision-making, better risk identification, gaining value, resource allocation, improved compliance, and corporate governance. The Standard's risk management process is presented in Exhibit 1.

27. The Guidance document takes each element of the risk management process in Exhibit 1 and elaborates on that step. For example, for the step "establishing the context," the commentary focuses on understanding an organization's objectives and its external and internal stakeholders. As another example, the Guidance provides commentary on "criteria" for establishing the context, which include the kinds of consequences and the definition of likelihood. The commentary on criteria further includes detailed case examples of criteria and the related objectives.

COSO's Enterprise Risk Management—Integrated Framework

28. COSO published in 1992 *Internal Control—Integrated Framework*, and in 2004, followed with publication of an ERM framework (see Exhibits 2 and 3). As noted previously in paragraph nine, the COSO definition of ERM is very broad. The ERM framework is clearly distinct from COSO's internal control framework. Interestingly, despite being more current, the SEC requires that companies comply with COSO's internal control framework rather than the ERM framework in meeting the SOX 404 requirements. The ERM framework notes that internal control is a part of ERM.

29. The COSO ERM framework has eight interrelated components (see Exhibit 3). According to COSO's ERM framework, internal environment refers to the tone of the organization, its risk appetite and elements such as oversight by the board. The framework states that companies must set objectives at the strategic level and must identify the risks and opportunities that impact the entity. Risks must then be assessed, and a response to the risk made—avoidance, reduction, sharing, or possibly acceptance. Clearly, COSO's ERM framework is one of the most comprehensive frameworks.
30. COSO also published “application techniques” to supplement the framework. This document provides examples to assist companies in implementing ERM. For example, related to the internal environment component, the application techniques document shows sample risk management philosophy statements and illustrative codes of conduct. Other examples are given for each of the framework's components.

IMA's Collaborative Assurance and Risk Design— Management Edition
(CARD-ME)

31. The IMA has announced its intention to develop a risk framework, noting that SOX 404 compliance is too costly and is potentially causing some companies to de-list as a way to avoid implementing SOX. Furthermore, SOX is currently seen as an

initiative that pulls top management away from value and strategy and leads to making the U.S. less competitive. The IMA stated that current frameworks are not focused sufficiently on risks but rather emphasize audit or control issues.

32. The IMA framework will be a “management centric” risk framework and is called *Collaborative Assurance and Risk Design – Management Edition (CARD-ME)*. This framework should provide assistance in meeting what Congress called for in the SOX Act. Once the framework is published, companies should be able to avoid the excessive emphasis on documenting and testing controls and instead be able to put their efforts on risk and control for value. In other words, management will know the right amount of control rather than building controls to meet checklists. The framework is basically an “enterprise risk approach” that will allow companies to build cost-effective controls with management taking the lead in setting controls rather than auditors.

VII ERM FOUNDATIONAL ELEMENTS

33. While a variety of ERM frameworks have been suggested by different professional organizations and consulting firms, the essential components of most frameworks are similar. They differ in the language used to describe the components in the ERM process as well as in the number of specific steps. In implementing ERM, a company may want to adapt a generic framework to fit its culture, management philosophy, capabilities, needs, industry, and size. This section discusses the organizational context for ERM and the basic components in a generic ERM framework.

Organizational Context

34. An effective ERM implementation requires an organizational context that includes:

- the tone at the top;
- risk management philosophy and appetite;
- integrity and ethical values; and
- scope and infrastructure for ERM.

The Tone at the Top

35. A pre-condition for effective ERM implementation is the tone set by the board of directors and top management, who are ultimately responsible for risk management. A board with a majority of independent directors should regularly seek from executive management responses to these questions: “What are the company’s top risks and what are you doing to manage them?” The board discussion around these questions sends a message to top management that the board recognizes that any organization is vulnerable to risk, and they expect top management to maintain an effective risk management process. In turn, the importance that top management places on effective ERM in its decisions sends a message to the entire organization.

Risk Management Philosophy and Risk Appetite

36. How the organization views risks and considers it in decisions is the core of a company's risk management philosophy. Management seeks to create value by growing the company, and the risk management philosophy serves as a control over which risks are acceptable in pursuing growth opportunities.
37. An organization's risk management philosophy is manifested in its risk appetite, which reflects how much risk the company can optimally handle given its capabilities and the expectation of its various stakeholders. The company's capabilities in terms of the core competencies of its people, technology, and capital are key determinants of the amount of risk it can take overall. The company's risk appetite influences its culture, strategic decisions, and operating style. The company's stakeholders—shareholders, executives, employees, and others—have expectations concerning the organization's appropriate amount of risk, and thus, they also influence the setting of the risk appetite. Companies should understand and be fully aware of the risk appetite of all stakeholders.
38. While risk appetite is a broad, entity concept, risk tolerance has a narrower focus. An organization may have different risk tolerances for its various operating units, but when the individual risk tolerances are combined, they should fall within the overall risk appetite set by top management and the board.

Integrity and Ethical Values

39. Management's uncompromising commitment to integrity and ethical behavior in all areas of decision making are prerequisites to implementing effective ERM. If employees sense that management is cutting corners and not setting an example for acceptable behavior, they will likely follow suit and develop the same attitude about right and wrong and put the organization's reputation at risk. An organization's reputation takes years to build but can be diminished quickly by unethical behavior. Reputation risk is recognized as one of the major risks that organizations must proactively manage.
40. Formal codes of conduct that are constantly reinforced through training programs serve to set boundaries for all employees as to what is unacceptable behavior. Under SOX, the SEC was directed to set rules that require a company to disclose if it has adopted a code of ethics, and if it does not have one, to explain why. This disclosure requirement enhances the internal environment supporting ERM implementation.

Scope and Infrastructure for ERM

41. In launching an ERM initiative, the scope of the effort should be clearly stated. Some organizations have rolled out the ERM effort initially in a specific operating unit and beta tested the framework they were using before implementing it across the company. In addition, a decision must be made on the risk infrastructure. Will the effort be overseen by a chief risk officer, an ERM advisory committee, or some combination of both? A chief risk officer supported by a cross-

functional risk advisory committee is one approach. Regardless of the approach, risks identified are owned by the operating units, not the chief risk officer or a committee. Also, the ERM effort will not succeed without champions at the C-level supporting the risk infrastructure.

Basic Components of ERM Framework

42. The basic components found in most ERM frameworks are (see Exhibit 4):
- set strategy and objectives;
 - identify risks;
 - assess risks;
 - treat risks;
 - control risks; and
 - communicate and monitor.

Set Strategy and Objectives

43. The first step in the ERM framework requires an understanding and clarity of strategy and objectives. The opportunities that a company decides to pursue are articulated in its strategy and objectives. Risks are the events or actions that jeopardize the achievement of the strategy and related objectives. The identification of risk is dependent upon clarity of objectives for the unit under analysis, which might be the overall organization, a strategic business unit, a function, an activity, a process, or a reporting and compliance requirement.

44. One of the benefits derived from ERM is that in the implementation process it may be revealed that some objectives are not really clear and understood by those responsible for achieving them. Employees may not understand how their daily jobs and tasks relate to the objectives. Some companies have found they have had to devote effort at this point clarifying the unit's objectives before they can move to the next step of identifying risks. ERM requires companies to state objectives clearly at every level of the organization where risks are identified.

Identify Risks

45. A list of techniques available for identifying risks is presented in Exhibit 5. (These techniques are discussed in the SMA on *Tools and Techniques of Enterprise Risk Management*). The goal in identifying risks is to produce a comprehensive list of risks and to assess them, narrowing the list to the top risks facing the organization. In selecting from the list of techniques, a consideration is the rigor of the technique and will it encourage openness among the participants. Because of the diversity and complexity of risks, using several of the techniques on the list may be required to ensure that as many risks as possible are identified. If some risks fail to be identified in the process, they may later lead to a major problem for the organization or a missed opportunity. At the end of the risk identification process, the company should have its own list of risks—the organization's risk language—with an agreement on the meaning of each one.

Assess Risks

46. Once risks have been identified, risk assessment is the next step. A key to ERM is to know the risks the company can control and those over which it has little or no control. A second and related key is to know which risks can be measured and those that cannot be measured. Knowing the importance of a risk through risk assessment can lead to better management and resource allocation. Further, knowing how that risk interrelates with other risks in the organization can enhance ERM. A 2005 survey by Protiviti indicated that companies are using a variety of approaches in implementing ERM:

- 39% do risk assessment workshops;
- 32% do risk modeling;
- 30% have risk-based metrics; and
- 28% do risk mapping.

Risks must be assessed or measured in some way, and the variety of approaches available from qualitative to quantitative are presented in Exhibit 6.

47. When a risk is identified, the implication is that it has some significance and can be ranked on some scale of importance. An example of a subjective assessment of risk and related rankings is provided in Exhibit 7. In a risk assessment workshop, each participant can rank the risk previously identified on a 1 to 3 scale, and the risks can be sorted by the rankings. Management can then focus on those risks that have been ranked as the most important.

48. Risks can also be assessed using a low, medium, or high level of impact or significance. Alternatively, risks can be assessed using a dollar level of impact. In addition to the impact or significance of risks, the probability of a risk occurring should be considered. Once impact and probability are determined, a risk map can be generated as illustrated in Exhibit 8.
49. Risk maps can be more detailed as shown in Exhibit 9 by breaking down impact into categories or dollar amount measured by a selected metric. The annualized impact can be measured in terms of some metric such as earnings per share or net income. The probability can also be expanded into categories such as greater than 90% chance, 30 to 60% chance, or less than 10% chance of the risk event occurring.
50. Some companies display risk in zones on maps designated by color as shown in Exhibit 10. A risk in the green zone indicates low dollar impact and probability of occurrence, the yellow zone indicates moderate risk, and the risks with the highest impact and likelihood are in the red zone.
51. An advantage of risk maps in colored zones is that companies that have assessed risks across the enterprise can display the colors and compare the risk assessments in a report. For example, the report in Exhibit 11 shows how each risk is assessed across the enterprise by every function or division. Resolving differences in risk assessments and seeking possible risk solutions can lead to valuable discussions.

Other quantitative analysis and risk tools are discussed in the SMA on *Tools and Techniques of Enterprise Risk Management*.

52. When placing risks on a map, the risks can be presented based on the inherent assessment, which is the level of risk in the event before any mitigation decision. Residual risk is that remaining after management has taken mitigation action. Risk maps can also be presented showing the residual risk. As an example, a company identified numerous risks as part of its risk identification process. One of the key risks was financial risks. However, the company's executives and internal auditors believed strong controls were already in place for the identified financial risks. Therefore, their residual risk was low in this area, and the company chose to focus on another of the top risks identified.

Treat and Control Risks

53. After risks are identified and assessed, management must decide how to respond to them. One of the goals of ERM should be to make conscious decisions about risk. The actions that management might take for a given risk include: avoidance, reduction, sharing, and acceptance. Management determines its response to a risk by considering the effect a given decision will have on impact and likelihood of the risk and what the costs and benefits are of its action. The goal is to take actions that will bring the organization's overall residual risk within the entity's risk appetite. As noted in paragraph 38, risk tolerances may vary but overall they should fall

within the risk appetite approved by executive management and the board. Linking inherent and residual risk with risk tolerance is illustrated in Exhibit 12. In this analysis, the first risk analyzed was the number of available qualified candidates. The company identified several related risks and then adopted a risk management strategy. Through its action, management concluded the likelihood of the risk was reduced from 20% to 10%.

54. To respond properly and treat a risk, companies must also source the risk to the root causes. For example, a grain company identified weather as a risk. After studying the risk, the company decided the risk to manage was not weather, but grain volume. Many things affected grain volume besides weather, such as loss of product in shipping and handling and waste. Similarly, a company identified an earthquake as a risk. After studying the earthquake risk thoroughly, the company decided that they needed to focus on several related risks. For example, the company's buildings could be earthquake secure but their suppliers' buildings or employees' homes may not be safe. Other related and critically important risks were how a potential earthquake would affect customer service, research and development on new products, and expansion into new markets. The destruction of the physical facilities in an earthquake had far-reaching implications that had to be analyzed.
55. Treating and controlling risks can take a variety of actions. To mention several actions, companies can implement new policies and controls, purchase derivatives,

hire new management, or implement new training programs. This variety of risk treatment approaches is why ERM is a much broader concept than financial reporting and internal control risk. Of course, companies can still just accept and bear the risk. For example, some airlines have more aggressive approaches to managing the risk of fuel price increases and decreases than do others.

56. An insurance and financial services company discovered its sales force had slowly become out of control. To promote sales, the sales force had developed their own training material that was not authorized by the company. The sales force was increasingly dishonest with customers by telling them to ignore notices from the company about premiums, and they were asking customers to sign blank withdrawal forms which allowed the sales team to withdraw funds from the customers' accounts. Simultaneously, the company also faced risks related to industry trends that were indicating a shrinking market in one of their key product areas. It is probable that the broader industry trends and declining market were the root cause of the pressure on the sales force and marketing areas. The company responded by hiring a new CEO with expertise in areas into which the company wanted to expand. Additionally, the company adopted new sales and marketing policies to control the risk of the sales force misleading customers by using unauthorized advertising and training material. The company also implemented customer support lines to help resolve disputes with customers and engaged independent industry organizations to verify with customers that they were knowledgeable about what they had purchased.

Communicate and Monitor

57. Organizations are generally involved in distributed risk taking in that each operating unit faces risk in pursuing their profit objectives and goals to grow their piece of the business. The desired outcome for ERM is that organizations not become risk adverse but that risk-based decision making is fostered at all levels of the organization, where managers take risk knowingly and by intention utilizing appropriate risk information. Accordingly, communication of risk related information must flow down, across, and up the organization. As illustrated previously in Exhibit 11, summary reports of risk assessments at the division or function level provide senior management with valuable information on how the top risks facing the organization are viewed by middle management.
58. Ongoing monitoring occurs in well managed organizations as a normal course of conducting business. Under ERM monitoring is enhanced by incorporating information on risk identification and assessment and identifying the owners of specific risks. Monitoring is discussed further in the next section.

VIII. INTEGRATING ERM IN ONGOING MANAGEMENT ACTIVITIES

59. The business environment is constantly changing and as a consequence implementing ERM is a never ending process. Sustaining ERM requires constant attention by C-level executives, and integration into on-going management

initiatives sends a message to associates at all levels of its importance. When ERM is seen as sound business management rather than “the management fad of the month,” it becomes an integral part of the organization’s “DNA.” Some of the opportunities for integrating ERM in on-going management activities include:

- strategic planning;
- balanced Scorecard (BSC);
- budgeting;
- business continuity (crisis management);
- corporate governance; and
- risk disclosures.

Strategic Planning

60. The COSO definition of ERM cited previously in paragraph nine states that ERM is part of strategy setting. ERM and strategy setting should be viewed as complimenting each other and not as independent activities. If strategy is formulated without identifying the risks embedded in the strategy and assessing and managing those risks, the strategy is incomplete and at risk of failing. Similarly, if ERM does not begin with identifying risks related to the company’s strategy, the effort will be incomplete by failing to identify some very important risks.

Mismanagement of strategic risks has been shown to be the cause for loss of major shareholder value.²

61. In the process of formulating the company's strategy, top management analyzes its strategic alternatives, identifying events that could threaten their achievement. As the risks embedded in each strategic alternative are identified and placed on a risk map the alternative can be evaluated against the organization's capabilities and how it aligns with the risk appetite. Some strategies might be outside the risk appetite of the company and a decision is made not to pursue them—a decision to avoid the risk. Other strategies may be very risky but can be managed and monitored carefully and thus will be pursued—a decision to accept the risk. Another strategy may be risky but the decision is made to pursue it through a joint venture—a decision to share the risk. Still another alternative strategy with considerable risk embedded in it might be pursued incrementally— a decision to reduce the risk. Strategy formulation is enhanced by ERM because risks are identified, and the strategic alternatives are assessed given the company's risk appetite. In turn, without a well articulated strategy, the foundation for implementing ERM is

² Two studies have pointed out the significant loss of shareholder share that resulted from the mismanagement of strategic risks. A study by Mercer Management Consulting analyzed the value collapses in the *Fortune* 1000 during the period 1993-1998. The analysis found that 10% of the *Fortune* 1000 lost 25% of shareholder value within a one-month period. Mercer traced the collapses back to their root causes and found that 58% of the losses were triggered by strategic risk, 31% by operational risk, 6% by financial risk, and hazard risk did not cause any of the decrease in shareholder value. (*Enterprise Risk Management – Implementing New Solutions*, 2001; 8.) A more recent study by Booz Allen Hamilton analyzed 1200 firms during the period of 1999 through 2003 with market capitalizations greater than \$1 Billion. The poorest performers were identified as companies that trailed the lowest-performing index for that period, which was the S&P 500. The primary events triggering the loss of shareholder value were strategic and operational failures. Of the 360 worst performers in the study, 87% of value destruction suffered by these companies related to strategic and operational mismanagement. (Kocourek, 2004: 1.)

insufficient. Viewing the two together forms the basis for a strategy-risk-focused organization.

Balanced Scorecard (BSC)

62. The BSC is a tool for communicating and cascading the company's strategy throughout the organization. The conventional BSC captures the company's strategy in four key perspectives:

- customer;
- internal;
- innovation and learning; and
- financial.

63. Integration of the BSC with ERM can enhance performance management. In the BSC, objectives are identified for each of the perspectives, and as noted previously, ERM begins with an understanding of objectives. For each BSC perspective, metrics (key performance indicators—KPI's) are selected and stretch targets are set. ERM adds value to the BSC through the identification of events (risks) that could stand in the way of achieving the targets in each of the four perspectives. By monitoring the KPI's, management can assess how effectively their risk mitigation efforts are working. In effect, the KPI's for each perspective also serve as key risk indicators (KRI's) although they are not initially selected for that purpose. For example, if a target for customer satisfaction is not achieved, it suggests that some

risks related to the item exist. The same metric can be used for monitoring both strategy and risk.

64. The conventional BSC can be integrated with ERM to manage and monitor risk related to the strategic objectives. Using a risk scorecard for the key risks identified in each of BSC perspectives is a way to assign responsibility for managing the risk. As shown in Exhibit 13, the special risk scorecard begins with the articulation of the specific objectives for the particular perspective. Next, for each of those objectives, the key risks are identified along with the suggested control processes. The focus area identifies the risks as strategic, operational, or financial. Management's self assessment of its risk mitigation actions is shown in the worksheet by asking: "Is it in place? If so, how effective is it?" The last column focuses on identifying the owner of the risk who will be held accountable for managing it. A risk scorecard, if maintained on the company's intranet, allows management to review the scorecard at any time, which adds strength to the accountability for the management of the risk.

Budgeting

65. A company's budget or financial plan reflects this year's initiative to implement the organization's long-term strategy. The annual budget can be integrated with ERM to provide insights on what the strategic business unit's leadership sees as the threats to meeting its financial plan. In the conventional budgeting process, the

leadership of the strategic business unit presents its profit plan to senior management, who probe and ask questions to uncover the risks implicit in the numbers.

66. A risk map presented with the unit's budget provides information to senior management on what the major threats are to meeting the financial plan for the year. The risk map gives senior management a point of departure in the budget review process, without having to waste time uncovering the implicit budget risks. Operating units should know their risks if they are to have any chance of accomplishing the plan. An additional benefit of including a risk map on the budget risks is that as the various budgets and risk maps are reviewed by senior management, they can compare the risks they have identified in the strategic plan with those identified by the operating units. Any disparities in how the two groups perceive the risks facing the organization can be further analyzed.

67. When a risk map accompanies the budget, senior management can ask questions about the expenses in the budget that relate to risk mitigation decisions for the high impact/high likelihood risks (the red zone risk in Exhibit 10). Also, if a decision was made not to mitigate certain risks, it is important to understand the impact on the unit's cost structure by taking that action. Another relevant issue is to understand to what extent the cost of mitigating or accepting a risk has been built into the price of the product or service. ERM coupled with the budget review

process can enrich a discussion and lead to a better understanding of the threats standing in the way of making budget.

Business Continuity (Crisis Management)

68. As noted in the previous discussion of risk identification, regardless of how robust that effort is, some unknown risks will remain unknown at the end of the process. A company prepares for these unknown risks through its business continuity or crisis management plan, which is an essential element of the ERM process.
69. A crisis is a point at one end of a continuum with risks at the other end. With the Internet-based new media like bloggers, message boards, chat rooms, e-mailing lists, and independent news Web sites, a company must be prepared to recognize a crisis and respond swiftly to contain it before damage is done to its reputation and brands. A company will need to “play war games” to test the crisis management plan and to ensure that all the key employees know their roles. In addition, communication with the entire work force about the plan in advance of a crisis is an essential part of the preparation.
70. When a crisis occurs, it does not evolve in a linear way because if it is not recognized quickly and if efforts are not made to contain it, a series of reactions and events in other areas either within and/or outside the organization may be triggered. Exhibit 14 shows the “triggering or ballooning” impact of a crisis and how it may

develop exponentially. As an example, a major company sold some contaminated product in two countries, which caused some users to become ill. A failure by the company to recognize the crisis quickly led the governments of the two countries to pull the product from store shelves. After some delay, the CEO traveled from the U.S. to the countries and eventually apologized publicly. However, the damage was done as the company's stock price fell and eventually the CEO was replaced.

Corporate Governance

71. ERM ties in closely with corporate governance by:

- improving information flows between the company and the board regarding risks;
- enhancing discussions of strategy and the related risks between executives and the board;
- monitoring key risks by accountants and management with reports to the board;
- identifying acceptable levels of risks to be taken and assumed;
- focusing management on the risks identified;
- improving disclosures to stakeholders about risks taken and risks yet to be managed;
- reassuring the board that management no longer manages risk in silos; and
- knowing which of the organization's objectives are at greatest risk.

72. As noted in the list above, the flow of risk information to the board is critically important in improving corporate governance. A major U.S. retailer presents its risk maps to its audit committee of the board to keep them fully informed. They also communicate to the audit committee their action plans for the risks and how they monitor those risks. Finally, they inform the audit committee on how the risk assessment and metrics used to monitor the risk relate to shareholder value measurements.
73. Another example of how risk information enhances corporate governance is from a not-for-profit organization, which analyzes risks by division and by the top 100 executives. The results of this risk analysis is discussed with the organization's board and top executives, who also use the risk information as an input into their strategic planning. This organization identifies any risks over a materiality level or risk tolerance level and requires automatic reporting to the board as well as development of an action plan by the division manager who owns that risk.

The Board and Stock Exchanges

74. The corporate governance rules of the NYSE, which were approved by the SEC on November 4, 2003, incorporate elements of risk assessment and management into the listing requirements. The NYSE rules state that it is the responsibility of the audit committee to discuss the company's policies with respect to risk assessment and risk management. In commentary on this requirement, the governance rules

note that the job of the CEO and senior management includes assessing and managing risk. Additionally, the NYSE rules state that the audit committee of the board should discuss policies with the CEO and senior management that govern the risk process.

75. NASDAQ also issued new rules of governance for listed companies, which were approved by the SEC. NASDAQ stated that their goals for corporate governance enhancement included empowering shareholders and enhancing disclosure. NASDAQ's corporate governance requirements address distribution of reports, independent directors, audit committees, shareholder meetings, quorums, solicitation of proxies, conflicts of interests, shareholder approval, stockholder voting rights, and code of conduct. However, NASDAQ did not incorporate risk or an ERM process into its listing requirements.

Risk Disclosures

76. Companies are increasingly disclosing more information about the risks they face. In some instances, this risk information is the result of new regulatory requirements, and in others, it is a management decision.

Proxy Statements

77. Currently, no disclosures are required in proxy statements about risk management infrastructure, processes, or management and board responsibility in the area of risk. However, disclosure of the audit committee charter may mention “business risk and control” and indicate that the audit committee should ask the following groups about significant risks: executive management, the CFO, and the independent accountant.

Management’s Discussion and Analysis (MD&A)

78. “Meaningful disclosures” was the purpose of the 2003 guidance by the SEC on the MD&A section of the 10-K. According to the SEC, a good MD&A section should help an investor see material opportunities, challenges, and risks for both the short-term and long-term. Further, the company should discuss actions taken related to these opportunities and risks. The SEC added that this information may not necessarily be accounting information but might instead be nonfinancial information. Nonfinancial information related to opportunities and risks could be key indicators, key variables, time-to-market, information on customer satisfaction, information on employee retention, or on business strategy. The enterprise risk management process and the management accountant could be a valuable source for gathering this information.

10-K Item 1A— Risk Factor Disclosure

79. Effective December 1, 2005, SEC rules mandate “risk factor disclosure” in a new item 1A of the company’s Form 10-K. Companies are also required to issue quarterly updates for material changes in the risk factors. The SEC noted that some companies already disclose some risk related to forward looking statements. However, the SEC is mandating every company explicitly identify risk factors. The risk factor disclosures are to be based on “an evaluation of the material risks facing the issuer.” As such, companies have to know and evaluate their risks. The SEC believes these new disclosures are not too much of a burden because companies will already have internal controls over financial reporting and disclosure controls and procedures in place.

Other Voluntary Disclosures

80. Even if the above disclosures are made by companies, this does not mean that a company manages its risks. Boards, shareholders and other stakeholders should want to know more about a company’s ERM process. This applies to public or private organizations.
81. Some companies disclose publicly that they have an ERM process. Other companies disclose that they have a risk committee, a chief risk officer, or the risk infrastructure. Still others disclose software they are using in ERM. A biotech

company discloses key process/operational risks in addition to other risk factors and how those risk fit into ERM. They further disclose how they are measuring and managing that risk.

IX. TRANSITIONING FROM SOX TO ERM

82. To comply with SOX companies have incurred additional costs internally, and audit fees have increased as auditors attempt to opine on management's assessment of the entity's internal controls. As a result of these additional costs, arguments have been made that companies will either de-list if already public, never go public, or consider going public overseas. However, these approaches are shortsighted. Stronger internal controls, better corporate governance, and implementation of ERM can lead to improved stability, reaction time, and increased shareholder value.
83. Companies that have implemented the SOX Act and Section 404 have learned how to identify important financial statement accounts and disclosures, how to design effective control systems, and how to test those systems. They have also learned that excessive controls can be just as bad as no controls. Section 404 requires a company identify and manage the risks related to financial reporting. Audit committees have now become accustomed to discussing these financial reporting risks.
84. Audit committees and the entire board should now take the next step and expand

into ERM. There is even more to be gained by managing all risk, not just financial reporting risk. Given that most financial reporting failures are business failures first, it should come as no surprise that ERM can not only add shareholder value but can also lead to better communication with stakeholders and possibly reduced business failures.

X. CONCLUSION

85. ERM is a powerful management tool that is never completed and requires champions at the C-level for its successful implementation. In today's risky world, companies can no longer rely on a silo approach to risk management but need an integrated and holistic perspective of all the risks facing the organization. A risk-centric organization does not avoid risks but rather knowingly takes risks aligned with its risk appetite.

86. Integration of ERM with ongoing management activities serves to embed risk management throughout a company. As company's implement ERM, some best-practices are presented in Exhibit 15. ERM is not an option in today's business environment where companies are required to disclose risk factors in the financial reports, and the board of directors regularly questions top management about the company's risk.

GLOSSARY

Impact – The significance of a risk to an organization. Impact captures the importance of the risk. Impact can be measured quantitatively or qualitatively.

Inherent Risk – The level of risk that resides with an event prior to management taking mitigation action.

Likelihood – An estimate of the chance or probability of the risk event occurring.

Opportunity – The upside of risks.

Residual Risk – The level of risk that remains after management has taken action to mitigate the risk.

Risk – Any event or action that can keep an organization from achieving its objectives.

Risk Appetite – The overall higher level of risk an organization is willing to accept given its capabilities and the expectations of its stakeholders.

Risk Tolerance – The level of risk an organization is willing to accept around specific objectives. Risk tolerance is a more narrow level than risk appetite.

BIBLIOGRAPHY

Augustine, N. R. "Managing the Crisis You Tried to Prevent." *Harvard Business Review* (November-December 1995): 147-158.

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

Barton, T. L., W. G. Shenkir, and P. L. Walker. *Making Enterprise Risk Management Pay Off*. Upper Saddle River, NJ: Financial Executives Research Foundation, 2001.

Barton, T. L., W. G. Shenkir, and P. L. Walker. "Managing Risk: An Enterprise-wide Approach." *Financial Executive* (March-April 2001): 48-51.

Bernstein, P. L. *Against the Gods — The Remarkable Story of Risk*. New York: John Wiley & Sons, Inc., 1996.

Bodine, S., Pugliese, A, and P. L. Walker. "A Road Map to Risk Management." *Journal of Accountancy*, December, 2001.

Brancato, Carolyn. *Enterprise Risk Management: Beyond the Balanced Scorecard*. New York: The Conference Board, 2005.

Burns, Judith, "Everything You Need to Know About Corporate Governance..." *The Wall Street Journal* (October 27, 2003): R6.

Byrne, John, "Joseph Berardino (Cover Story)." *Business Week* (August 12, 2002): 51-56.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). *Internal Control—Integrated Framework: Executive Summary Framework*. New York: AICPA, 1992.

---, *Enterprise Risk Management—Integrated Framework: Executive Summary Framework*. New York: AICPA, 2004.

---, *Enterprise Risk Management – Integrated Framework: Application Techniques*. New York: AICPA, 2004.

Corporate Executive Board. *Confronting Operational Risk – Toward an Integrated Management Approach*. Washington, DC: Corporate Executive Board, 2000.

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

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

Economist Intelligence. *Managing Business Risks –An Integrated Approach*. New York: The Economist Intelligent Unit, 1995.

--- *Enterprise Risk Management —Implementing New Solutions*. New York: The Economist Intelligent Unit, 2001.

Emen, Michael S. *Corporate Governance: The View from NASDAQ*. NASDAQ: 2004.

Epstein, Marc J and Adriana Rejc. *Identifying, Measuring, and Managing Organizational Risks for Improved Performance*. Society of Management Accountants of Canada and AICPA, 2005.

Federation of European Risk Management Associations. *A Risk Management Standard*. 2003.

Financial and Management Accounting Committee of the International Federation of Accountants (IFAC), prepared by PricewaterhouseCoopers. *Enhancing Shareholder Wealth by Better Managing Business Risk*. New York: International Federation of Accountants, 1999.

Financial Reporting Council. *The Combined Code on Corporate Governance*. 2003.

Financial Reporting Council. *Internal Control: Revised Guidance for Directors on the Combined Code*. 2005.

Gates, Stephen and Ellen Hexter. *From Risk Management to Risk Strategy*. New York: The Conference Board, 2005.

Gibbs, Everett and Jim DeLoach. "Which Comes First...Managing Risk or Strategy-Setting? Both." *Financial Executive* (February 2006): 35-39.

Hands On. "Risk Management Issues for Privately Held Companies." *ACC Docket* (May 2006): 76-88.

King Committee on Corporate Governance. *King Report on Corporate Governance for South-Africa*. Institute of Directors in Southern Africa, 2002.

Institute of Management Accountants. "IMA Announces Bold Steps to 'Get it Right' on Sarbanes-Oxley Compliance. Press release: December 21, 2005.

Joint Standards Australia/ Standards New Zealand Committee. *Risk Management*. Standards Australia/Standards New Zealand, 2004.

Joint Standards Australia/Standards New Zealand Committee, *Risk Management Guidelines*. Standards Australia/Standards New Zealand 2004.

Kaplan, Robert S., and David P. Norton. "The Balanced Scorecard—Measures that Drive Performance." *Harvard Business Review* (January-February 1992): 71-79.

Kaplan, R. S., and D. P. Norton. "Putting the Balanced Scorecard to Work." *Harvard Business Review* (September-October 1993): 134-147.

Kaplan, Robert S., and David P. Norton. *The Balanced Scorecard*. Harvard Business School Press, 1996.

Kaplan Robert S., and David P. Norton. *The Strategy-Focused Organization*. Harvard Business School Press, 2001.

Kocourek, Paul, Reggie Van Lee, Chris Kelly, & Jim Newfrock, "Too Much SOX Can Kill You." *Strategy+Business* (Reprint, January 2004): 1-5.

"Living Dangerously: A Survey of Risk." *The Economist* (January 24, 2004):1-15.

McNamee, D., and G. M. Selim. *Risk Management: Changing the Internal Auditor's Paradigm*. Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation, 1998.

Miccolis, J. A., K. Hively, and B. W. Merkley. *Enterprise Risk Management: Trends and Emerging Practices*. Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation, 2001.

Nagumo, T. "Aligning Enterprise Risk Management with Strategy through the BSC: The Bank of Tokyo-Mitsubishi Approach." *Balanced Scorecard Report* (Harvard Business School Publishing, Reprint No. B0509D, September-October 2005):1-6.

---, and Barnby S. Donlon. "Integrating the Balanced Scorecard and COSO ERM Framework." *Cost Management* (July/August 2006): 20-30.

National Association of Corporate Directors. *Report of the NACD Blue Ribbon Commission of Audit Committees —A Practical Guide*. National Association of Corporate Directors, 1999.

New York Stock Exchange. *Final NYSE Corporate Governance Rules*. November 4, 2003.

Nottingham, L. *A Conceptual Framework for Integrated Risk Management*. The Conference Board of Canada, 1997.

Protiviti. *U.S. Risk Barometer—Survey of C-Level Executives with the Nation’s Largest Companies*. 2005.

Sarbanes-Oxley Act of 2002. H.R. 3763.

Schwartz, Peter. *The Art of the Long View*. New York: Currency Doubleday, 1991.

Shenkir, W. and Paul L. Walker. “Enterprise Risk Management and The Strategy-Risk-Focused Organization.” *Cost Management* (May-June 2006): 32-38.

Shaw, Carl. “Internal Controls.” *Strategic Finance* (March 2006): 6.

Simons, Robert L. “Control in an Age of Empowerment.” *Harvard Business Review* (March-April 1995): 80-88.

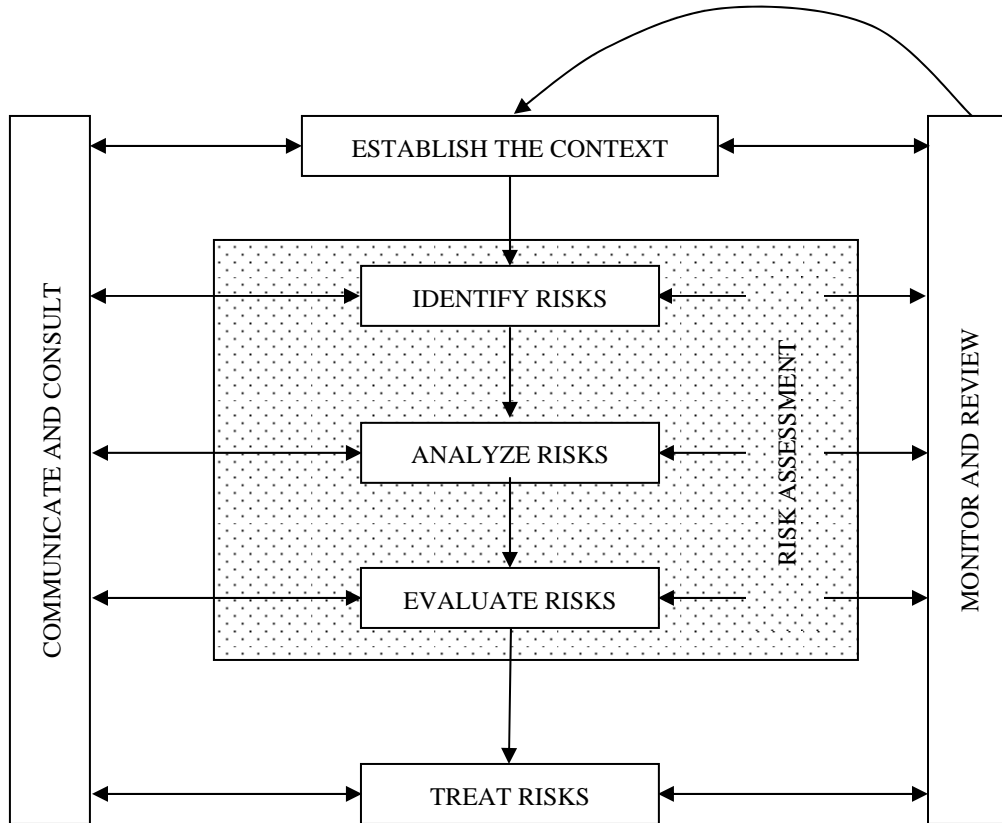
Simons, Robert. L. “How Risky Is Your Company?” *Harvard Business Review* (May-June 1999): 85-94.

Smith, Carl L. “The Trouble with COSO.” *CFO.com* (March 15, 2006):1-4.

Smith, Wendy K. “James Burke: A Career in American Business (A) (B).” Harvard Business School Case 9-389-177 and 9-390-030. Harvard Business School Publishing, 1989.

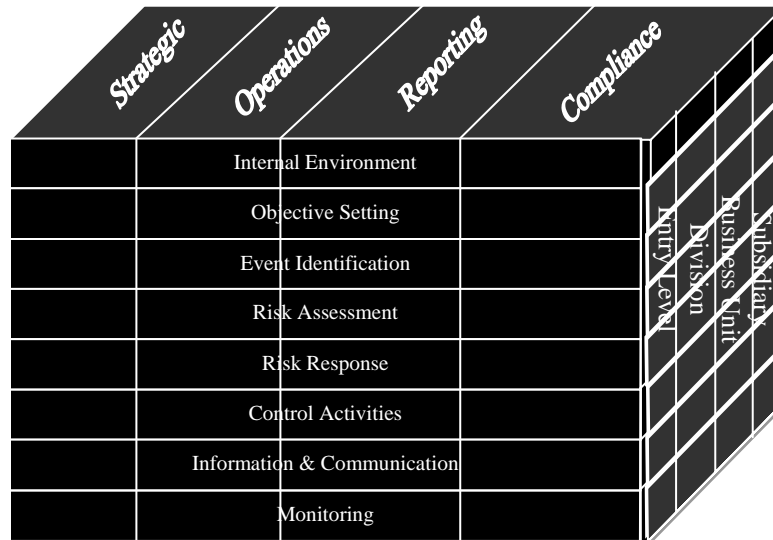
- Slywotzky, Adrian J. and John Drzik. "Countering the Biggest Risk of All." *Harvard Business Review* (Reprint R0504E, April 2005): 1-12.
- Thornton, Emily. "A Yardstick for Corporate Risk." *Business Week* (August 26, 2002): 106-108.
- Treasury Board of Canada Secretariat. *Integrated Risk Management Framework*.
Treasury Board of Canada Secretariat, 2001.
- , *Integrated Risk Management Framework: A Report on Implementation Progress*
Treasury Board of Canada Secretariat, 2003.
- U.S. Securities and Exchange Commission, Commission Guidance Regarding
Management's Discussion and Analysis of Financial Condition and Results of
Operations, Release No. 33-8350, December 19, 2003.
- U.S. Securities and Exchange Commission, Securities Offering Reform, Release No. 33-
8591, Effective December 1, 2005.
- Walker, P. L., W. G. Shenkir, and T. L. Barton. *Enterprise Risk Management: Pulling It
All Together*. The Institute of Internal Auditors Research Foundation, 2002.
- Walker, P. L., W. G. Shenkir, and T. L. Barton. "ERM in Practice." *Internal Auditor*
(August 2003): 51-55.
- Walker, P. L., W. G. Shenkir, & S. Hunn. "Developing Risk Skills: An Investigation of
Business Risks and Controls at Prudential Insurance Company of America. *Issues in
Accounting Education* (May 2001): 291-304.

Exhibit 1: Australia/New Zealand Standard—Risk Management Process—Overview



Source: Joint Standards Australia/Standards New Zealand Committee, *Risk Management*, 2004:9

Exhibit 2: COSO Enterprise Risk Management Framework



Source: *Enterprise Risk Management—Integrated Framework: Executive Summary Framework*, 2004:7.

Exhibit 3: COSO Enterprise Risk Components

Internal Environment

Risk Management Philosophy – Risk Appetite – Board of Directors – Integrity and Ethical Values – Commitment to Competence – Organizational Structure – Assignment of Authority and Responsibility – Human Resource Standards

Objective Setting

Strategic Objectives – Related Objectives – Selected Objectives – Risk Appetite – Risk Tolerances

Event Identification

Events – Influencing Factors – Event Identification Techniques – Event Interdependencies – Event Categories – Distinguishing Risks and Opportunities

Risk Assessment

Inherent and Residual Risk – Establishing Likelihood and Impact – Data Sources – Assessment Techniques – Event Relationships

Risk Response

Evaluating Possible Responses – Selected Responses – Portfolio View

Control Activities

Integration with Risk Response – Types of Control Activities – Policies and Procedures – Controls Over Information Systems – Entity Specific

Information and Communication

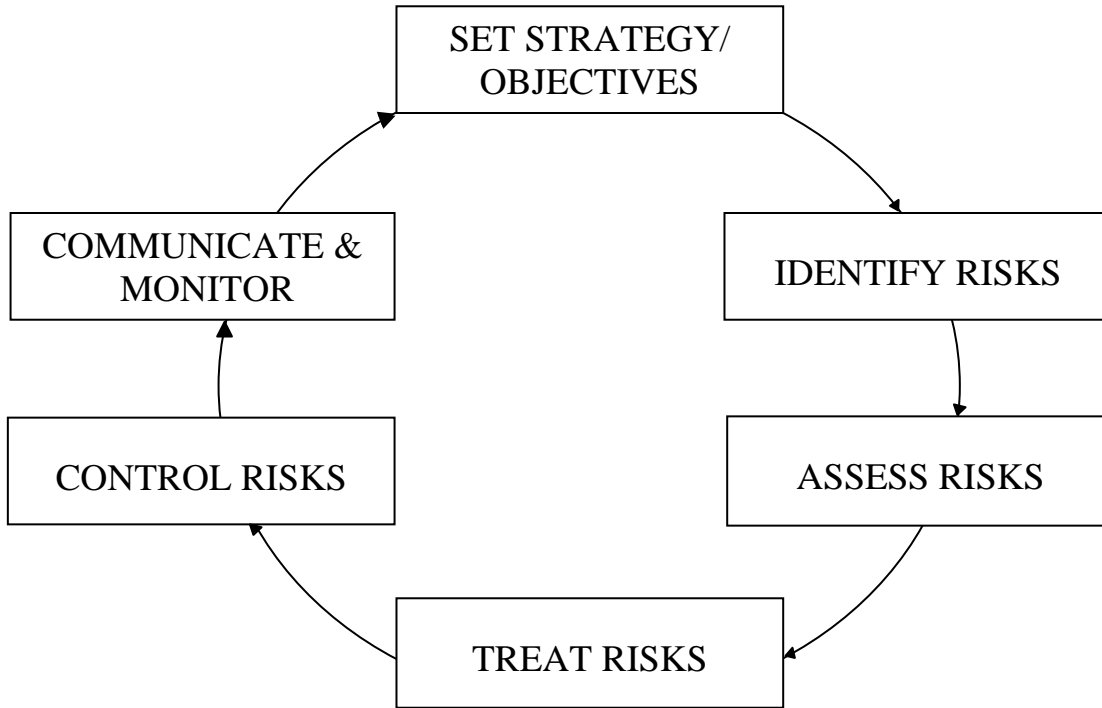
Information – Communication

Monitoring

Ongoing Monitoring Activities – Separate Evaluations – Reporting Deficiencies

Source: *Enterprise Risk Management—Integrated Framework: Application Techniques*, 2004:2.

Exhibit 4: A Continuous Risk Management Process



Source: Adapted from The Institute of Chartered Accountants in England & Wales, 1999:47.

Exhibit 5: Risk Identification Techniques

Internal interviewing and discussion:

- interviews
- questionnaires
- brainstorming
- Self-assessment and other facilitated workshops
- SWOT analysis (strengths, weaknesses, opportunities, and threat

External sources:

- comparison with other organizations
- discussion with peers
- benchmarking
- risk consultants

Tools, diagnostics and processes:

- checklists
- flowcharts
- scenario analysis
- value chain analysis
- business process analysis
- systems engineering
- process mapping

Source: AICPA, *Managing Risks in the New Economy*, 2000: 9.

Exhibit 6: Risk Quantification and Qualitative Techniques

Qualitative and Quantitative Approaches to Assessment and Measurement

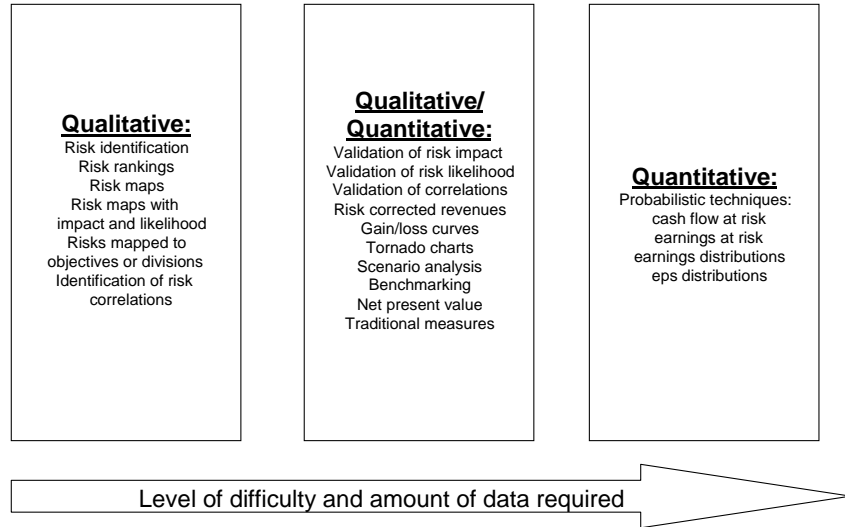


Exhibit 7: Subjective Assessment of Risk

Brainstorming Output

	Survey Responses															Total
Risks:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Score
Sample Risk #1	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	17
Sample Risk #2	2	1	1	1	2	1	1	1	1	1	1	1	1	2	1	18
Sample Risk #3	2	1	2	1	2	1	2	1	1	1	1	1	1	1	1	19
Sample Risk #4	3	1	1	1	1	1	1	1	2	2	2	1	1	1	1	20
Sample Risk #5	3	1	2	1	1	2	1	2	1	2	1	1	1	1	1	21
Sample Risk #6	2	1	1	1	2	2	1	1	2	2	1	1	1	1	2	21
Sample Risk #7	3	2	3	1	1	1	1	1	2	1	2	1	2	1	1	23
Sample Risk #8	2	2	2	1	2	2	2	1	1	1	1	1	1	2	2	23
Sample Risk #9	3	2	1	1	2	2	1	1	2	1	1	2	2	2	2	25
Sample Risk #10	2	2	3	2	1	2	3	3	3	2	1	2	3	2	1	32

1 = very important

2= somewhat important

3 = not important

Exhibit 8: Risk Map

High

**Impact on
Achievement
of Objectives
(Significance)**

High Impact Low Likelihood	High Impact High Likelihood
Low Impact Low Likelihood	Low Impact High Likelihood

Low

Likelihood of Occurrence

High

Exhibit 9: Risk Map

Risk Map							
	?		Probability of Occurrence				
Critical	> \$15 M	5					
High	\$10–15 M	4					
Moderate	\$5–10 M	3					
Low	\$1–5 M	2					
Not Significant	< \$1 M	1					
Annualized impact measured in terms of ? Probability measured over a one year time horizon			1	2	3	4	5
			< 10%	10 – 30%	30 – 60%	60 – 90%	> 90%
			Slight	Not Likely	Likely	Highly Likely	Expected

Exhibit 11: Functional Risk Assessment Summary

Corporate Risk Assessment 2000/2001		Function #1	Function #2	Function #3	Function #4	Function #5	Function #6	Function #7	Function #8	Function #9	Function #10	Function #11	Function #12	Function #13	Function #14	Function #15
Comparison of Functional Risk Assessments																
1: External Environment																
2: Customer (Internal & External) Needs																
3: Culture																
4: Operations																
5: Communications																
6: Security																
7: Human Resource																
8: Information availability/processing/technology																
9: Financial																
10: Legal/Compliance																
11: Management and monitoring of operation																

Source: *Enterprise Risk Management: Pulling It All Together*, 2002:45.

Exhibit 12: Linking Objectives, Events, Risk Assessment and Risk Response

Operations objective	<ul style="list-style-type: none"> Hire 180 new qualified staff across all manufacturing divisions to meet customer demand without overstaffing Maintain 22% staff cost per dollar order 				
Objective unit of measure	Number of new qualified staff hired				
Tolerance	165–200 new qualified staff, with staff cost between 20% and 23% per dollar order				
Risks	Inherent risk assessment		Risk response	Residual risk assessment	
	Likelihood	Impact		Likelihood	Impact
Decreasing number of qualified candidates available	20%	10% reduction in hiring → 18 unfilled positions	Contract in place with a third party hiring agency to source candidates	10%	10% reduction in hiring → 18 unfilled positions
Unacceptable variability in our hiring process	30%	5% reduction in hiring due to poor candidate screenings → 9 unfilled positions	Review of hiring process conducted every two years	20%	2% reduction in hiring due to poor candidate screenings → 4 unfilled positions
Alignment with risk tolerance	Response expected to bring company within risk tolerance				

Source: *Enterprise Risk Management—Integrated Framework: Application Techniques*, 2004:56.

Exhibit 13: Balanced Scorecard and Strategic Risk Assessment

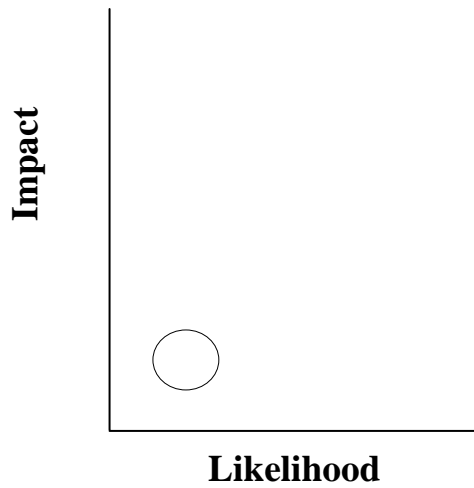
Exhibit 13: Balanced Scorecard and Strategic Risk Assessment									
Learning and Growth Objectives						Mitigation Process			
No.	Objective	Risk Number	Risk	Suggested Control Processes	Focus Area	In Place	Effectiveness*	Comments	Owner of Corrective Action

* Effectiveness Rating: 1 to 10, with 10 being very effective.

Exhibit 14: Risk/Crisis Acceleration

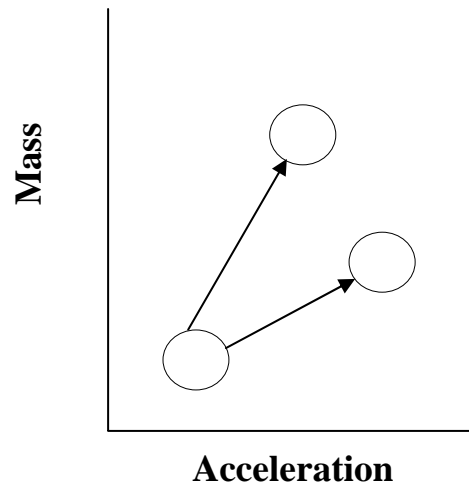
A.

Risk Occurrence



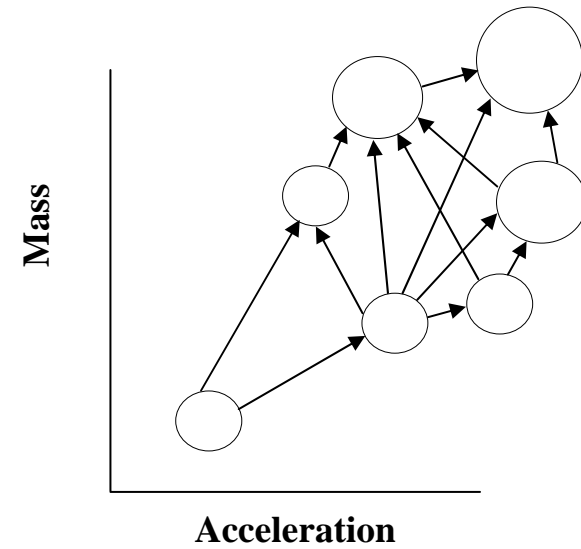
B.

**Crisis Occurrence –
Gathering Storm**



C.

**Crisis Occurrence –
Catastrophic Force**



Source: *Enterprise Risk Management: Pulling It All Together*, 2002:100.

Exhibit 15: Hallmarks of Best-Practice ERM

1. Engaged senior management and board of directors that set “the tone from the top” and provide organizational support and resources.
2. Independent ERM function under the leadership of chief risk officer (CRO), who reports directly to the CEO with a dotted line to the board.
3. Top-down governance structure with risk committees at the management and board levels, reinforced by internal and external audit.
4. Established ERM framework that incorporates all of the company’s key risks: strategic risk, business risk, operational risk, market risk and credit risk.
5. A risk-aware culture fostered by a common language, training and education, as well as risk-adjusted measures of success and incentives.
6. Written policies with specific risk limits and business boundaries, which collectively represents the risk appetite of the company.
7. An ERM dashboard technology and reporting capability that integrates key quantitative risk metrics and qualitative risk assessments.
8. Robust risk analytics to measure risk concentrations and interdependencies, such as scenario and simulation models.
9. Integration of ERM in strategic planning, business processes and performance measurement.
10. Optimization of the company’s risk-adjusted profitability via risk-based product pricing, capital management and risk-transfer strategies.

Source: James Lam & Associates Inc., *Financial Executive*, January/February 2005:38.