ima®

The Association of Accountants and Financial Professionals in Business

Enterprise Risk Management: Frameworks, Elements, and Integration

Statement on Management Accounting

About IMA® (Institute of Management Accountants)

IMA, named 2017 Professional Body of the Year by *The Accountant/International Accounting Bulletin,* is one of the largest and most respected associations focused exclusively on advancing the management accounting profession. Globally, IMA supports the profession through research, the CMA® (Certified Management Accountant) program, continuing education, networking, and advocacy of the highest ethical business practices. IMA has a global network of more than 100,000 members in 140 countries and 300 professional and student chapters. Headquartered in Montvale, N.J., USA, IMA provides localized services through its four global regions: The Americas, Asia/Pacific, Europe, and Middle East/India. For more information about IMA, please visit www.imanet.org.

Statements on Management Accounting

SMAs present IMA's position on best practices in management accounting. These authoritative monographs cover the broad range of issues encountered in practice.

Institute of Management Accountants
10 Paragon Drive, Suite 1
Montvale, NJ, 07645
www.imanet.org/thought_leadership

About the Authors

Paul L. Walker, Ph.D., CPA, is the James J. Schiro/Zurich Chair in Enterprise Risk Management and executive director at the Center for Excellence in ERM at St. John's University. Paul co-developed one of the first courses on enterprise risk management (ERM) and has done ERM training for executives and boards around the world. He has written extensively on risk and ERM including the books *Improving Board Risk Oversight through Best Practices*, *Making Enterprise Risk Management Pay Off*, and *Enterprise Risk Management: Pulling it All Together.* He was a consultant to COSO on its ERM framework. He taught at the University of Virginia and has served as a visiting fellow at the London School of Economics Centre for the Analysis of Risk and the University of Canterbury at Christchurch.

William G. Shenkir, Ph.D., CPA, is the William Stamps Farish Professor Emeritus at the University of Virginia's McIntire School of Commerce, where he served on the faculty and as dean. Bill has co-authored research studies on enterprise risk management (ERM) funded by five different professional organizations. He also served as a consultant to COSO on its 2004 ERM project, co-developed a graduate ERM course in 1996, and has spoken on ERM before numerous professional groups in the United States and abroad. He served as president of the Association to Advance Collegiate Schools of Business International (AACSB) and as a vice president of the American Accounting Association (AAA).

Table of Contents

Table of Exhibits

I. The Case For Enterprise Risk Management

Leadership is about making a difference. If leaders of organizations in the 21st 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.

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 stakeholder value. The need for greater risk awareness by leaders is driven by much more than just cyber threats. Forces such as globalization and the geopolitical environment in which organizations operate add complexity to business, thereby increasing risks. Disruption, innovation, technology, and Big Data require companies to rethink their business models, core strategies, and target markets. Customers have ever-increasing demands for customized products and services, 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 deregulation in others, both of which drive risks. Mergers and restructurings are causing organizations to downsize and undergo changes in management responsibilities, which also creates the potential for enterprise risks. Given all of these forces, leaders must have a heightened state of awareness of the necessity for holistic risk management and for a stronger governance structure for their organization.

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 and trends in performance indicators. The general assumption was that executive management had its eye on the big picture of strategic risks facing the enterprise in the short term and over the life of the strategic plan.

As organizations grow in complexity and serve global markets, the leadership challenge is to understand fully how the various organizational 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 it strives to identify, assess, and manage risks and, when taking risks, the leadership does so intentionally rather than unknowingly. The key is to take calculated risks across the enterprise and appropriately manage and mitigate the risks for the benefit of the stakeholders.

II. Defining Risk and ERM

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 a mix of both risk and opportunity. In the 2017 publication *Enterprise Risk Management—Integrating with Strategy and Performance,* the Committee of Sponsoring Organizations of the Treadway Commission (COSO) stated that ERM is, "The culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value." Several points to emphasize from this broad definition include:

- Risk management should be viewed as a core competency; and
- It's part of everyone's job—whether at the level of setting the organization's strategy, or a unit's objectives, or running the daily operations.

Organizations seek to create value for their stakeholders, and ERM is implemented with that goal in mind. Accordingly, ERM is:

> a structured and disciplined approach: It aligns strategy, processes, technology, and knowledge with the purpose of evaluating and managing the uncertainties the enterprise faces as it creates value.…It is a truly holistic, integrated, forward-looking, and process-oriented approach to managing all key business risks and opportunities—not just financial ones—with the intent of maximizing shareholder value as a whole.[1]

The authors of this Statement on Management Accounting (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." Given that ERM is applicable to all types of organizations, as noted below, some might prefer to use the term "stakeholder value" in this definition instead of "shareholder value."

III. Scope

This SMA provides an overview of the ERM process and 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, not-for-profit, or private entities. The information in this SMA provides management accountants and others interested in 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;

[1] James W. DeLoach, *Enterprise-wide Risk Management: Strategies for Linking Risk and Opportunity*, Financial Times, London, England, 2000.

- 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 ongoing management activities; and
- Ideas for adding value to the Sarbanes-Oxley (SOX) 404 compliance requirement by employing a risk-based approach to identify, test, and document key internal controls to assure investors on the quality of the firm's financial statements and related disclosures.

The information in this SMA provides an overview for an organization considering implementation of ERM. This document is not intended to provide a comprehensive discussion of ERM. Other sources, such as those identified in the bibliography, should also be consulted.

IV. Total Risk Classification

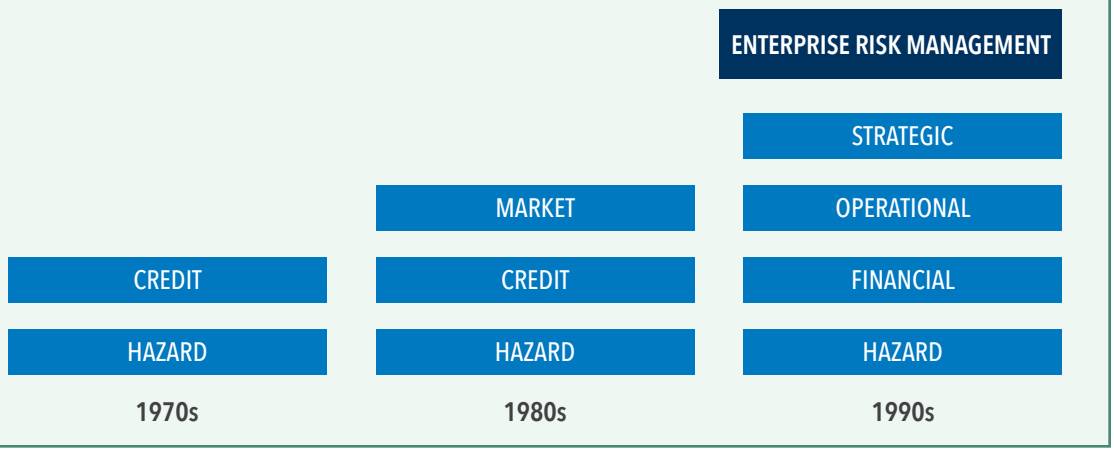
Taking the perspective of the total entity, risks may be classified in a variety of risk frameworks. Frequently used frameworks are:

- **Strategic Risks:** 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 human resources, business processes, technology, business continuity, channel effectiveness, customer satisfaction, health and safety, environment, product/service failure, efficiency, capacity, and change integration.
- **Financial Risks:** include risks from volatility in foreign currencies, interest rates, and commodities; also could include credit risk, liquidity risk, and market risk.
- **Hazard Risks:** risks that are insurable, such as natural disasters; various insurable liabilities; impairment of physical assets; terrorism.[2]

As noted in Exhibit 1, traditional risk management generally focused on financial risk and hazard risk. Approaching risk from an enterprise-wide perspective began to be considered and implemented in the 1990s. This holistic risk approach should enable management to identify most of the key risks that confront the organization. Implementing ERM, however, does not mean that an organization will be able to anticipate every risk that could result in loss of stakeholder value. The limitation of ERM is captured in the aphorism: "There are known knowns, known unknowns, and unknown unknowns." In the ERM process, known risks will be identified and some previously unknown risks will become known. Even with a robust process, however, 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 affect the organization negatively. Alternatively, unknown risks can create unique opportunities, and companies must be ready to capitalize on those opportunities.

[2] Paul L. Walker, William G. Shenkir, and Thomas L. Barton, *Enterprise Risk Management: Pulling it All Together,* The Institute of Internal Auditors Research Foundation, 2002.

EXHIBIT 1: EVOLUTION OF RISK MANAGEMENT



V. The Role of the Management Accountant

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 (CROs) or established executive-level risk committees, which may report directly to the board of directors audit committee, thereby enhancing their independence and importance. The ERM initiative gains momentum when it is strongly supported by the board of directors and audit committee. Executive management cannot merely begin the process and then move 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." Education in the ERM framework, the language of risk, and the value of proactive risk management is an imperative for successful ERM deployment. The 2006 Oversight Systems "Financial Executive Report on Risk Management" shows that companies are embracing the concept of ERM but continue to have difficulty with its implementation, noting that 68% of financial executives say their CEO is placing greater emphasis on the management of all types of risk on a holistic basis.[3] A 2017 ERM survey reports that 24% of organizations have a fully integrated ERM program in 2017 (up from 21% in 2013).[4]

It is important for executive management to communicate that it views 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

[3] Oversight Systems, "The 2006 Oversight Systems Financial Executive Report on Risk Management," 2006.
[4] Brandon Righi and Carol Fox, "2017 Enterprise Risk Management Benchmark Survey," 2017.

in getting general acceptance of ERM. It is important that executives set the tone at the top by calling for big-picture alignment, strong corporate governance, and risk educational programs.

The management accountant can make major contributions to moving the organization from silo risk management (or no meaningful risk management process at all) to an integrated and holistic approach. In the "new" era of the finance organization, in the migration from a *counter* of wealth to assisting in the *creation* of wealth (i.e., independent strategic business partner), the management accountant is increasingly being asked to serve on, if not lead, cross-functional teams to implement critical enterprise-wide initiatives. ERM provides a wealth of opportunities for the management accountant to help implement a disciplined, systematic process to maximize the value of the enterprise. Some specific activities where the skills and competencies of the management accounting professional can be useful in ERM implementation include:

- Serve as a champion for ERM, supporting 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 of the ERM process;
- Provide expertise to operational management on the organization's ERM framework and process;
- Serve on cross-functional and diverse ERM committees;
- Assist executive and operational management in analyzing and quantifying 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, and coach management in responding to risks;
- Design reports to monitor risks and develop financial and nonfinancial metrics to evaluate the effectiveness of risk mitigation (treatment) actions;
- Advise management on integrating ERM with the balanced scorecard (BSC) and budgeting process;
- Participate in development of business continuity (crisis management) plans;
- Advise on risk disclosures in the U.S. Securities & Exchange Commission (SEC) Form 10-K and the annual report;
- Serve as a champion for strong corporate governance incorporating ERM;
- Coach management on the value of extending SOX 404 compliance to encompass ERM, including business process owners and other operational functions conducting a holistic assessment of risks impacting achievement of their business objectives;
- Help the organization see the disruptive risks facing the company and how they are linked to the business model;

- Help the organization see, understand, and manage the risk in new innovation, products, and strategies;
- Develop a strong culture committed to being risk-aware and managing risk.

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 are aware of risk while doing their work and are held accountable for how they manage risks.

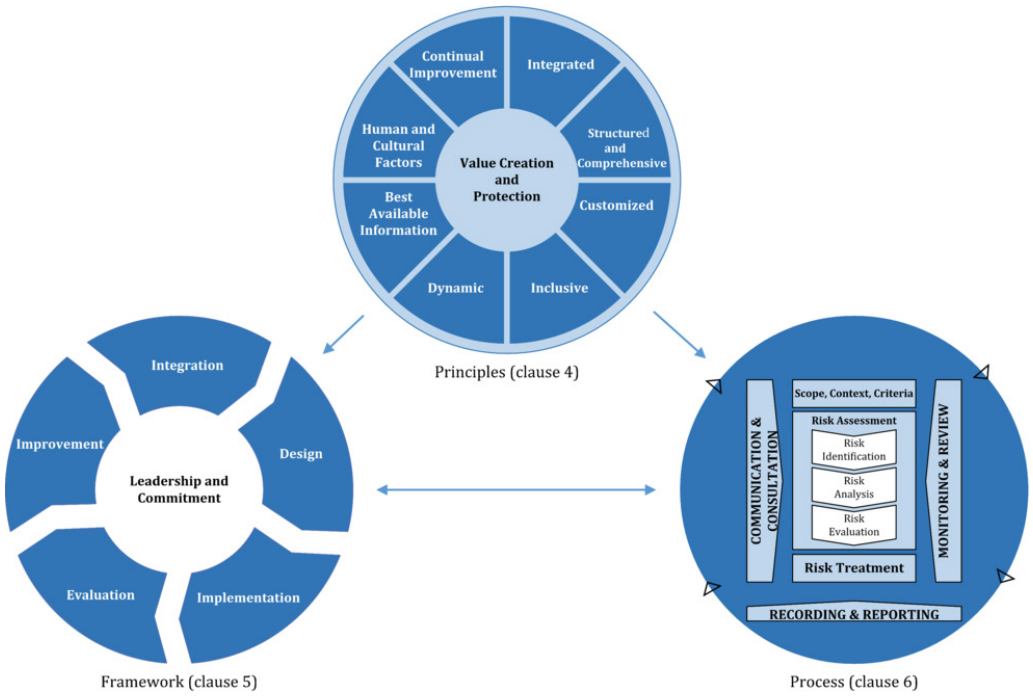
VI. ERM Frameworks

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. The two dominant and most widely used frameworks have been published by the International Organization for Standardization (ISO) and COSO.

ISO 31000 Risk Management—Principles and Guidelines

ISO issued its framework in 2009. It also issued a supporting standard document called ISO 31010:2009 that focuses on risk assessment techniques. A new ISO 31000 was published in 2018 (see Exhibit 2).

EXHIBIT 2: ISO 31000 RISK MANAGEMENT



The ISO guidance can be applied to any organization and is based on principles, a framework, and a process. The guidance notes that organizations may already have some of these components, but the need remains to adapt them to ensure risks are managed when setting strategy and achieving objectives, and when making informed decisions. The guidance's risk management process includes communication and consultation, monitoring and review, recording and reporting, scope and context, risk assessment, and risk treatment.

The *principles* are the characteristics of effective risk management and the *framework* is designed to help organizations integrate risk management into other (perhaps existing) functions or activities. The *process* is supposed to be integrated into the practices, policies, and so on, and be part of decision making. The process is applicable to all levels of an organization (from program all the way to strategy). The process is also designed to be iterative and to factor in the importance of culture throughout the entire process.

COSO's *Enterprise Risk Management—Integrating with Strategy and Performance*

COSO published its *Internal Control—Integrated Framework* in 1992. It followed that in 2004 with publication of its ERM framework, *Enterprise Risk Management—Integrated Framework.* That framework was updated in 2017 with *Enterprise Risk Management—Integrating with Strategy and Performance* (see Exhibits 3 and 4). As noted previously, the COSO definition of ERM is very broad. The ERM frameworks are clearly distinct from COSO's internal control framework. Currently, the SEC requires that companies attest in writing that their system of internal controls over financial reporting is effective in accordance with a "suitable" framework such as COSO's 1992 internal control framework. COSO considers the ERM framework to be much broader than internal control and controls over financial reporting. COSO has published additional ERM guidance on many topics including risk appetite, board risk oversight, and risk assessment.

The COSO ERM framework has five interrelated components (see Exhibit 3). The focus on the framework is on integration of risk management within the business activities and processes. That integration must be across mission, strategy, business objectives, performance, and value. It is not static. Again, COSO emphasizes that ERM includes the culture, capabilities, and practices of the organization.

EXHIBIT 3: COSO *ENTERPRISE RISK MANAGEMENT—INTEGRATING WITH STRATEGY AND PERFORMANCE* OVERVIEW

EXHIBIT 4: COSO *ENTERPRISE RISK MANAGEMENT—INTEGRATING WITH STRATEGY AND PERFORMANCE* COMPONENTS AND PRINCIPLES

The COSO ERM framework is supported by 20 principles that apply at different entity levels and across functions (see Exhibit 4), and each component has its own principles. As Exhibit 4 shows, the principles cover (among other things) areas such as:

- Exercises board risk oversight,
- Evaluates alternative strategies,
- Identifies risk,
- Reports on risk, culture, and performance.

The principles represent the keys behind each component.

The first component, Governance and Culture, is critical and sets the stage for the rest of ERM. It includes the principles (see Exhibit 4): exercises board risk oversight, establishes operation structures, defines desired culture, demonstrates commitment to core values, and attracts, develops, and retains capable individuals. Again, this component is the beginning and foundation for all the other components. COSO emphasizes that the tone is set here, the significance of ERM is established, and any necessary oversight responsibilities are put in place. Furthermore, management and the board should define the culture and desired behaviors and clearly establish the importance of culture and its influence on identifying risk, accepting risk, and managing risk.

Assessing ERM

Although it is certainly up for debate about any such legal or regulatory mandate for ERM across every industry, COSO has still provided a voluntary approach for assessing ERM that includes three considerations. First, to assess ERM, organizations could determine whether all components and relevant principles are present and functioning. Second, the components must be working in an integrated manner (not in silos). Third, necessary controls for the relevant principles must be present and functioning. Other organizations have developed ERM maturity models that can be used to gauge the progress of ERM.

Protiviti has a capability maturity framework that is designed to help management determine the maturity of its risk management by examining the risk management capabilities

for each risk type. Its approach also helps management decide the desired state as compared to the current state and then leads management toward actions to consider closing the gap. Deloitte also has a risk maturity model that includes stages such as: initial, fragmented, top down, integrated, and risk intelligent (the highest level). Each stage is built on a series of attributes that suggest an organization is in that stage. Deloitte argues that the key driver of risk maturity is management and the board's attitude about the "role and priority of risk management." Additionally, RIMS has a risk maturity model assessment tool that organizations can use to score their program by answering a series of questions designed to gauge certain risk attributes.

Standard & Poor's and ERM

Standard & Poor's (S&P) has already started to incorporate a company's ERM practice into the S&P rating of the company. S&P currently applies this rating to both financial institutions and insurers. Its framework for evaluating ERM at banks includes a review of ERM policies, ERM infrastructure, and ERM methodology. ERM policies should address risk culture, appetite, and strategy; control and monitoring; and disclosure and awareness. ERM infrastructure covers risk technology, operations, and risk training. ERM methodology refers to capital allocation, model vetting, and valuation methods.

The framework for evaluating insurers includes an assessment of risk management culture, risk controls, emerging risk management, risk and capital models, and strategic risk management. S&P has stated that the insurer is rated weak, adequate, strong, or excellent. An adequate rating would mean an insurer has "fully functioning risk control systems in place for all major risks."

VII. ERM Foundation Elements

While a variety of ERM frameworks has 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

An effective ERM implementation requires an organizational context that includes:

- Tone at the top;
- Risk management philosophy and risk appetite;
- Integrity and ethical values;
- Culture and ERM;
- Scope and infrastructure for ERM.

Tone at the Top

A necessary 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 executive management's responses to these questions: What are the company's top risks? What is its time horizon? What is being done 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 board members 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. Again, if the organization's risk committee and CRO report directly to the audit committee of the board of directors, this signals the importance of ERM.

Risk Management Philosophy and Risk Appetite

The core of a company's risk management philosophy is how it views risks and considers them when making decisions. 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. An organization usually cannot pursue all the numerous opportunities for growth that may be envisioned and must choose those that fall within its risk appetite and tolerance.

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 accept overall relative to business and stakeholder objectives. 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 if they wish to deliver optimal results.

While risk appetite is a broad, entity-wide 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. This is the essence of ERM, which is an integrated, holistic view of risks, in contrast with a silo approach to risk management. Additionally, risk mitigation under ERM takes an enterprise perspective rather than inefficiently mitigating risks independently.

Integrity and Ethical Values

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 manage proactively.

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 or explain why it has not. This disclosure requirement enhances the internal environment supporting ERM implementation.

Culture and ERM

While the ISO 2009 framework mentioned culture several times, the 2017 COSO ERM framework mentions culture more than 100 times. Additionally, there are two principles related to culture. Principle 3 is called "defines desired culture" and Principle 20 is called "Reports on risk, culture, and performance." Many organizations accept that culture is a key to success and greatness and must be more proactively managed. A study by IMA® (Institute of Management Accountants) on the Risk Challenge Culture added a new perspective that emphasizes that the culture and relationship between the board and C-suite must also be monitored and managed.[5]

Scope and Infrastructure for ERM

In launching an ERM initiative, the scope of the effort should be stated clearly. Some organizations initially rolled out the ERM effort 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 from a governance and leadership accountability perspective. Will the effort be overseen by a CRO, the CFO, an ERM advisory committee, or some combination? A CRO 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 CRO or a risk committee. Also, the ERM effort will not succeed without champions at the C-level supporting the risk infrastructure and a major, enterprise-wide education effort on the ERM methodology.

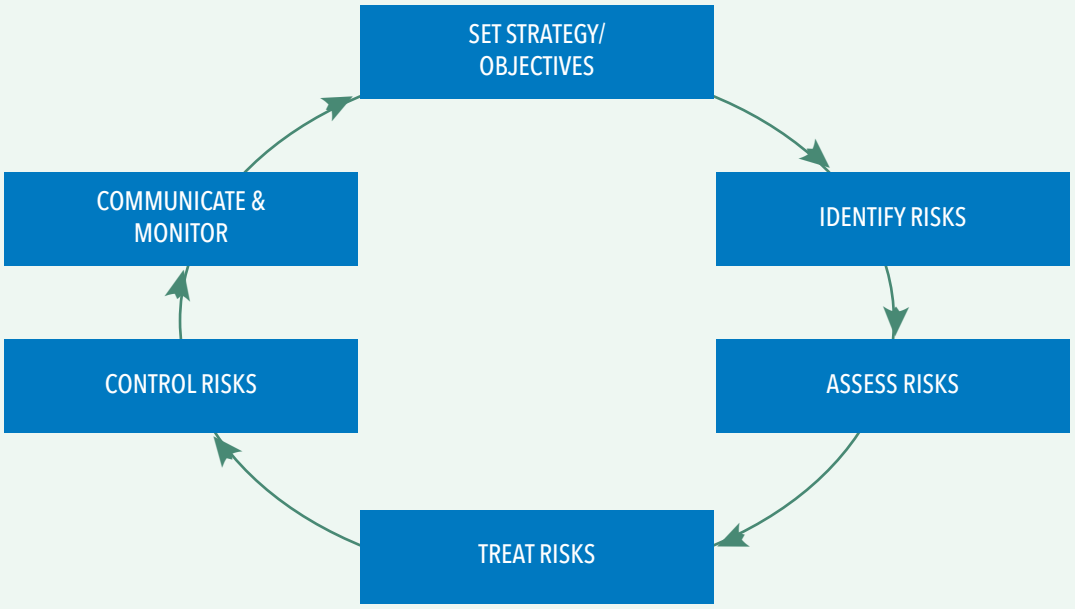
Basic Components of ERM Framework

The basic components found in most ERM frameworks are (see Exhibit 5):

- Set strategy and objectives,
- Identify risks,
- Assess risks,
- Treat risks,
- Control risks, and
- Communicate and monitor.

[5] Paul L. Walker, William G. Shenkir, and Thomas L. Barton, "A Risk Challenge Culture," IMA and ACCA, 2014.

EXHIBIT 5: A CONTINUOUS RISK MANAGEMENT PROCESS



Source: Adapted from The Institute of Chartered Accountants in England & Wales, *No Surprises: The Case for Better Risk Reporting,* ICAEW, London, U.K., 1999, p. 47.

Set Strategy and Objectives

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. On the upside, a holistic and proactive understanding of risk can lead to new or previously unidentified opportunities. The identification of risk is dependent on 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.

One of the benefits derived from ERM is that the implementation process may reveal that some objectives are not clear to all stakeholders or understood by those responsible for achieving them. Employees may not understand how their daily jobs and tasks relate to the objectives. At this point, some companies have found it necessary to devote effort in clarifying the unit's objectives before they can move on to the next step. ERM requires companies to state objectives clearly at every level of the organization where risks are identified—literally, from the workroom to the boardroom.

Identify Risks

A list of techniques available for identifying risks is presented in Exhibit 6. (These techniques are discussed in the SMA titled *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 down to the top risks facing the organization. When selecting from the list of techniques, the rigor of the technique and if it will encourage openness among the participants should be considered. 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 are identified as possible. If some risks fail to be identified in the process, it may later lead to a major problem for the organization or a missed opportunity. At the conclusion of the risk identification process, the company should have its own list of risks or risk language, with an agreement on the meaning of each one. This list is the organization's inherent risks, and once mitigation actions are determined, what remains are residual risks.

In identifying risks, one view is to start with a blank sheet of paper and develop the list of inherent risks by applying one or several of the techniques in Exhibit 6. Alternatively, a list of risks or a risk universe can be provided to those participating in the identification process. They, in turn, use this list to identify the risks relevant to the organization. Some combination of these two approaches also may be used to develop a comprehensive list of risks.

EXHIBIT 6: RISK IDENTIFICATION TECHNIQUES

Internal Interviewing and Discussion

- Interviews
- Questionnaires
- Brainstorming
- Self-assessment and other facilitated workshops
- SWOT analysis (strengths, weaknesses, opportunities, and threats)

External Sources

- Comparison with other organizations
- Discussion with peers
- Benchmarking
- Risk consultants

Tools, Diagnostics, and Processes

- Checklists
- Flowcharts
- Scenario analysis
- Business process analysis
- Systems engineering
- Process mapping

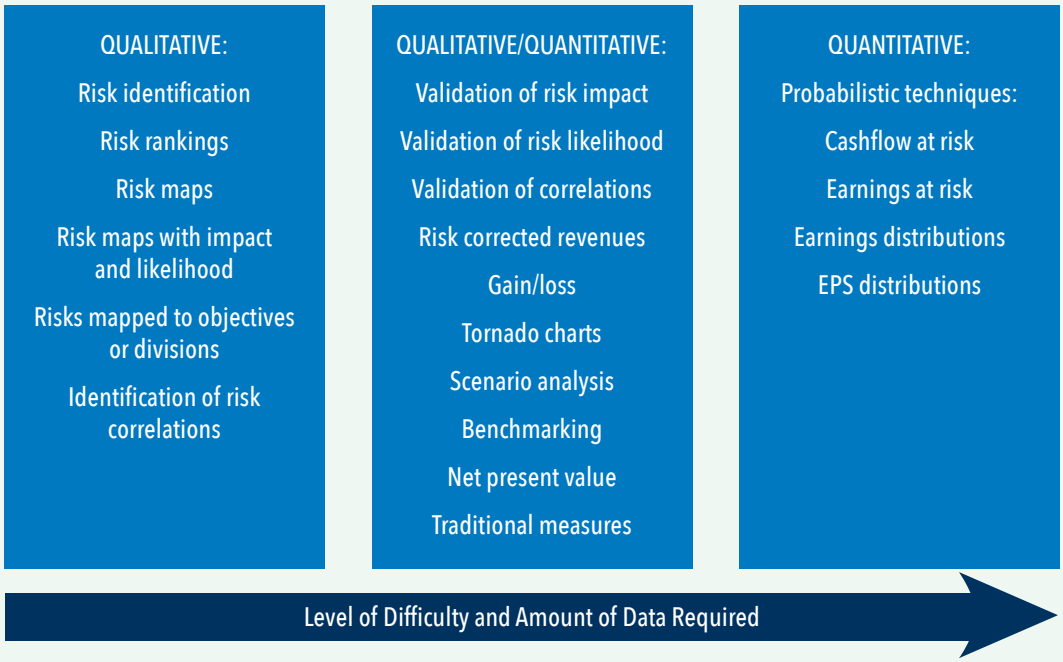
Source: American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA), *Managing Risk in the New Economy*, AICPA, New York, 2000, p. 9.

Assess Risks

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 and 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. COSO's ERM framework Principle 14 emphasizes that organizations develop a portfolio view of risks. Exhibit 7 presents the variety of approaches in implementing ERM available, from qualitative to quantitative.

EXHIBIT 7: RISK QUANTITATIVE AND QUALITATIVE TECHNIQUES

Qualitative and Quantitative Approaches to Assessment and Measurement



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 8. In a risk assessment workshop, each participant can rank the previously identified risk on a scale of 1 to 3, and the risks can be sorted by the rankings. Management can then focus on those risks that have been ranked as the most important.

EXHIBIT 8: SUBJECTIVE ASSESSMENT OF RISK

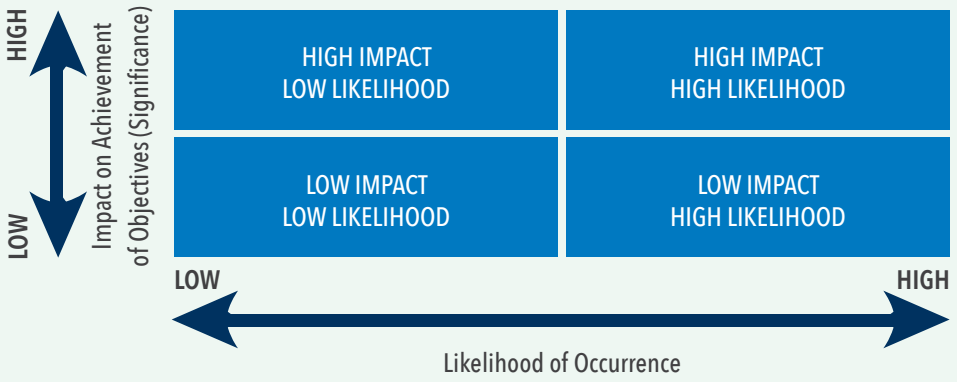
Brainstorming Output

	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

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. Other organizations determine impact using scales more relevant to their respective organization. For example, some define impact as the impact on reputation, safety, the environment, or compliance. 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 9.

EXHIBIT 9: RISK MAP



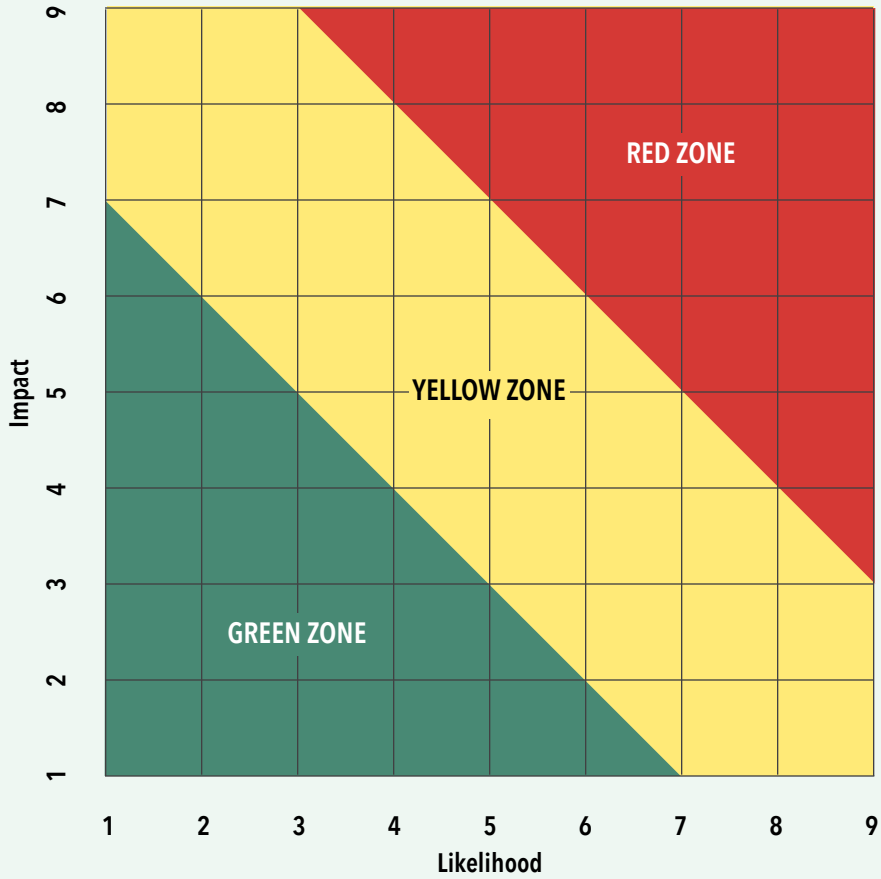
As shown in Exhibit 10, risk maps can be more detailed by breaking down the impact into categories or a dollar amount measured by a selected metric. The annualized impact can be measured in terms of some metric such as earnings per share or net income. The probability can also be expanded into categories such as greater than 90% chance, 30%-60% chance, or less than 10% chance of the risk event occurring.

EXHIBIT 10: DETAILED RISK MAP

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

Some companies display risk in zones on maps designated by color, as shown in Exhibit 11. A risk in the green zone indicates a 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.

EXHIBIT 11: COLOR-CODED RISK MAP

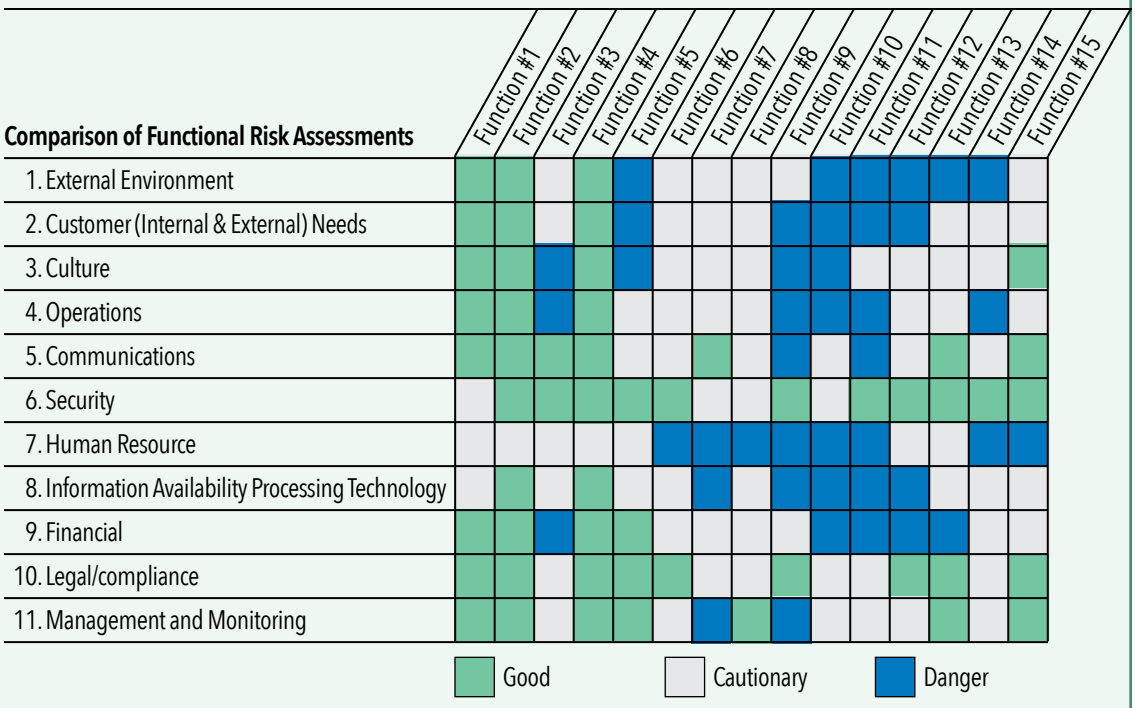


An advantage of risk maps with colored zones is that companies that have assessed risks across the enterprise can display the colors and compare the risk assessments in a report. For example, the report in Exhibit 12 shows how each risk is assessed across the enterprise by every function or division. Resolving differences in risk assessments and seeking possible risk solutions can lead to valuable discussions. Other quantitative analysis and risk tools are discussed in *Tools and Techniques of Enterprise Risk Management.*

When placing risks on a map, they can be presented based on the inherent assessment, which is the level of risk in each event before any mitigation action is taken. Residual risk is what remains after management has taken a 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, but the company's executives and

internal auditors believed that 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 other of the top risks identified.

EXHIBIT 12: FUNCTIONAL RISK ASSESSMENT SUMMARY



Source: Paul L. Walker, William G. Shenkir, and Thomas C. Barton, *Enterprise Risk Management: Pulling it All Together,* The Institute of Internal Auditors Research Foundation, 2002, p. 45.

Treat and Control Risks

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 impact a given decision will have, the likelihood of the risk, and the costs and benefits of its action. The goal is to take actions that will bring the organization's overall residual risk within its risk appetite. As noted previously, 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 13. 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%.

EXHIBIT 13: LINKING OBJECTIVES, EVENTS, RISK ASSESSMENT, AND RISK RESPONSE

Operations objective	• 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 screening →4 unfilled positions
Alignment with risk tolerance	**Response expected to bring company within risk tolerance**				

Source: COSO, *Enterprise Risk Management–Integrated Framework: Application Techniques,* New York, 2004, p. 56.

To respond and treat a risk properly, 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 it needed to manage was grain volume, not the weather. Many things affected grain volume besides weather, such as loss of product in shipping and handling or waste. Similarly, a company identified an earthquake as a risk. After studying the earthquake risk thoroughly, the company decided that it needed to focus on several related risks. For example, the company's buildings could be earthquake-secure, but its 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 by an earthquake had far-reaching implications that had to be analyzed.

Treating and controlling risks can require a variety of actions. For example, 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 if doing so is in alignment with their stakeholders' expectations. For example, some airlines have more aggressive approaches to managing the risk of fuel price increases and decreases than others.

An insurance and financial services company discovered its sales force had slowly become out of control. To promote sales, the sales force developed their own training material that was not authorized by the company. The sales force was increasingly dishonest with customers and told them to ignore notices from the company about premiums. Further, they asked 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 indicated a shrinking market in one of its 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

Organizations are generally involved in distributed risk taking as each operating unit faces risk in pursuing its profit objectives and goals to grow its piece of the business. The desired outcome for ERM is not that organizations become risk-averse, but that proactive, risk-based decision making is fostered at all levels of the organization and managers knowingly and intentionally take risk while utilizing appropriate risk indicators. Accordingly, communication of risk-related information must flow down, across, and up the organization. As illustrated in Exhibit 12, summary reports of risk assessments at the division or function level provide senior management with valuable information on how middle management views the top risks facing the organization.

Ongoing monitoring with key performance indicators (KPIs) and key risk indicators (KRIs) 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.

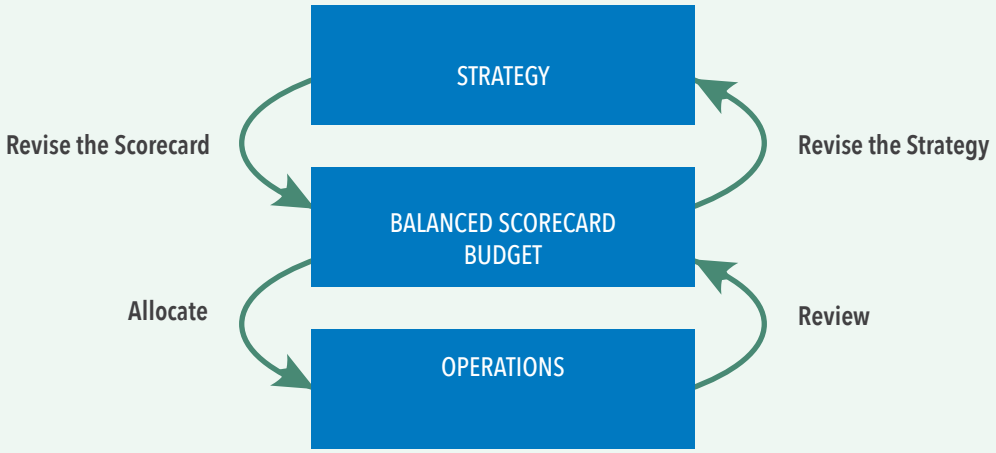
VIII. Integrating ERM into Ongoing Management Activities

The business environment is constantly changing. Consequently, implementing ERM is a continuous process much like the organization's strategy that ERM helps to achieve. Sustaining ERM requires constant attention by C-level executives, and integration into ongoing management initiatives stresses its importance to associates at all levels. 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 ongoing management activities include:

- Strategic planning;
- BSC;
- Innovation;
- Budgeting;
- Total quality management and Six Sigma;
- Business continuity (crisis management); and
- Corporate governance.

The relationship between strategic planning, the BSC, and budgeting is shown in Exhibit 14.

EXHIBIT 14: STRATEGY, THE BALANCED SCORECARD, AND THE BUDGET



Strategic Planning

The COSO definition of ERM states that ERM is part of strategy setting. ERM and strategy setting should be viewed as complementing 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 failure. Similarly, if ERM does not begin with

holistically 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, as pointed out by the following two studies:

> A study by Mercer Management Consulting analyzed the value collapses in the *Fortune* 1000 during 1993-1998.[6] 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, and 6% by financial risk. Hazard risk did not cause any of the decrease in shareholder value. Another study by Booz Allen Hamilton analyzed 1,200 firms during 1999-2003 with market capitalizations greater than $1 billion.[7] 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.

When formulating the company's strategy, top management analyzes its strategic alternatives and identifies 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 insufficient. Viewing the two together forms the basis for a strategy risk-focused organization. For example, the front end of the strategy formulation process is typically an environmental scan. Performed comprehensively, this scan reveals risks and opportunities.

BSC

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;

---

[6] Economist Intelligence Unit, *Enterprise Risk Management: Implementing New Solutions,* The Economist Intelligent Unit, New York, N.Y., 2001.

[7] Paul Kocourek, Reggie Van Lee, Chris Kelly, and Jim Newfrock, "Too Much SOX Can Kill You," *Strategy+Business,* Reprint, January 2004, pp. 1-5.

- Innovation and learning; and
- Financial.

Combining 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 (KPIs) 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 KPIs, management can assess how effectively their risk mitigation efforts are working. In effect, the KPIs for each perspective also serve as KRIs, 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.

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 the BSC perspectives is a way to assign responsibility for managing the risk. As shown in Exhibit 15, 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 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. Maintaining the risk scorecard on the company's intranet allows management to review the scorecard at any time, adding strength to the accountability for the management of the risk.

EXHIBIT 15: BSC 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.*

Similar to the BSC, some companies use strategy maps to capture the top four to five main areas that are important to the strategy. Risks can be traced back to the strategic areas to determine if there is a concentration around one specific strategic dimension.

ERM and Innovation

ERM can have a significant interaction with innovation in two ways. First, leading companies have learned to incorporate risk tools to help them understand the waves of disruption that might impact their business model. Identifying and understanding the risks that impact the business model must be done at the earliest possible time to enable an organization to manage possible downsides and to enable them to strategically position their organization to seize on the upside. Some risk tools used include value killer workshops, black swan workshops, strategic bow-tie analysis, game theory, opportunity workshops, and emerging risk analysis. One study noted that more than 90% of executives surveyed agreed that how well they anticipate, interpret, and react to market changes, trends, and disruption are keys to success. To stay successful, companies must increase their ability to see and understand the risky waves of change, and they must see those risks before it is too late.

ERM can also be used to make innovation more successful. Without a full understanding of the risk in new innovations, companies have already lessened the chances of success. Risk is not to be blindly taken. Many companies have adopted practices to incorporate ERM into innovation. For example, some companies mandate ERM team involvement in innovation based on some dollar threshold. Other companies have required ERM and risk acumen training to try to get the innovation teams to see the many risks as they are designing and developing new ideas and business models. Other approaches include risk post-mortems and risk-adjusting the numbers to incorporate the amount of risk and dimensions of risk. Building an innovation governance and BSC for innovation is another successful tool. Companies that learn to build ERM into innovation learn quickly that knowing the real risks means they can innovate more, manage the portfolio of risks better, and increase the chances of success for each innovation.

Budgeting

A company's budget reflects the current-year financial commitment to achieve 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, which probes and asks questions to uncover the risks implicit in the numbers.

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 analyzed further.

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 risks in Exhibit 11). If a decision was made not to mitigate certain risks, it also 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.

Total Quality Management and Six Sigma

Quality initiatives focus on improving the efficiency and effectiveness of detailed processes. ERM requires clarity of objectives at all levels of the enterprise, and the objectives of specific processes can be addressed by utilizing quality tools and methodologies. When an organization has implemented a quality initiative, information is available on detailed processes. In turn, this information can be evaluated within the larger context of the enterprise to identify risks in an ERM implementation. Also, quality initiatives can provide information on planning the mitigation action for a process risk. The process risk owner and source of the risks should be identified when implementing the quality initiative. This information should be insightful in treating the inherent risk with some control mitigation action. Once the control is implemented, the gap between the inherent risk and residual risk should be clearly evident.[8]

Business Continuity (Crisis Management)

Regardless of how robust an effort of risk identification 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—an essential element of the ERM process.

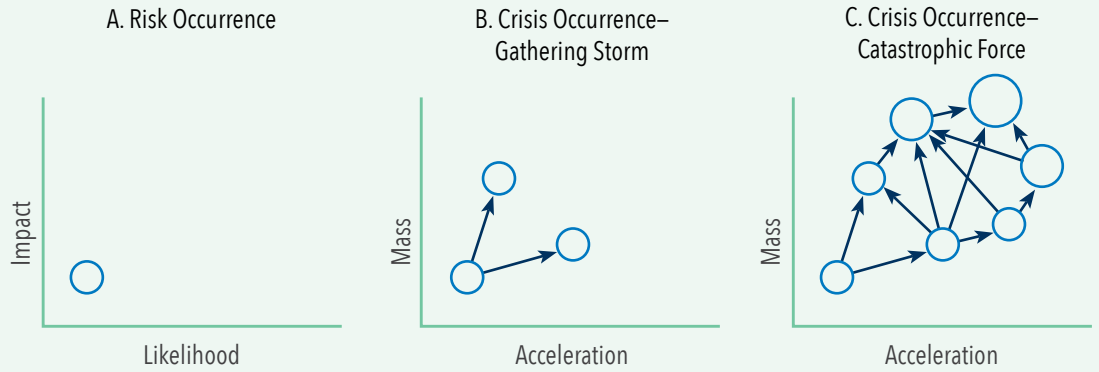
A crisis is a point at one end of a continuum, with risks at the other end. With internet-based new media like bloggers, message boards, chat rooms, email lists, and independent news websites, a company must be prepared to recognize a crisis and respond swiftly to contain it before damage is done to its reputation and brands. A company will need to "play war games" to test the crisis management plan and ensure that all the key employees know their roles. In addition, an essential part of the preparation is communication about the plan to the entire workforce in advance of a crisis.

When a crisis occurs, it does not evolve in a linear way: 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 16 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 that 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

[8] Protiviti, *Guide to Enterprise Risk Management,* 2006.

U.S. to the countries and eventually apologized publicly. The damage was done, however, as the company's stock price fell, and the CEO was eventually replaced.

EXHIBIT 16: RISK/CRISIS ACCELERATION



Source: Paul L. Walker, William G. Shenkir, and Thomas L. Barton, *Enterprise Risk Management: Pulling it All Together,* The Institute of Internal Auditors Research Foundation, 2002. This exhibit appears in the General Motors Case on page 100. At the time, Frederick Funston of Deloitte Enterprise Services was consulting with GM and created this illustration.

Corporate Governance

ERM ties in closely with corporate governance because it:

- Improves information flows between the company and the board regarding risks;
- Enhances discussions of strategy and the related risks between executives and the board;
- Monitors key risks and enables board risk reporting;
- Identifies acceptable levels of risks to be taken and assumed;
- Focuses management on the risks identified;
- Improves disclosures to stakeholders about risks taken and risks yet to be managed;
- Reassures the board that management no longer manages risk in silos; and
- Knows which of the organization's objectives is at greatest risk.

As noted in the list, the flow of risk information to the board is critical in improving corporate governance. For example, a major U.S. retailer presents its risk maps to its audit committee to keep the committee members fully informed. It also communicates to the audit committee its action plans for the risks and how those risks are monitored. Finally, it informs the audit committee on how the risk assessment and metrics used to monitor the risk relate to shareholder value measurements.

Another example of how risk information enhances corporate governance is from a not-for-profit organization. This entity 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

National Association of Corporate Directors (NACD) has issued guidance for boards related to risk oversight, and numerous best practices documents have been published.

Stock Exchanges and Regulatory Requirements

Stock Exchanges

The corporate governance rules of the New York Stock Exchange (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 audit committee's responsibility 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.

The NASDAQ exchange also issued new rules of governance for listed companies, which were approved by the SEC. NASDAQ stated that its 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 codes of conduct. NASDAQ did not incorporate risk or an ERM process into its listing requirements, however.

Board Risk Oversight Disclosures

Part of the increased emphasis by boards on ERM and risk oversight was caused by the SEC's board risk oversight proxy disclosure changes. The SEC rule was written in 2009 and required that companies disclose the board leadership structure, the board's role in risk oversight, and risk management and incentives linked to compensation policies. The SEC noted that risk oversight is a "key competence" of the board.

Management's Discussion and Analysis

"Meaningful disclosures" was the purpose of the 2003 guidance by the SEC on the Management's Discussion and Analysis (MD&A) section of Form 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 and long term. Further, the company should discuss actions taken related to these opportunities and risks. The SEC added that this information may not be accounting information necessarily, but it instead might be nonfinancial information. Nonfinancial information related to opportunities and risks could be key indicators, key variables, time-to-market, or information on customer satisfaction, employee retention, or business strategy. The ERM process and the management accountant could be a valuable source for gathering and reporting the potential implications of this information.

10-K Item 1A—Risk Factor Disclosure

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, but it is mandating that every company identify risk factors explicitly. 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 has a 2017 proposed rule to change the risk factor disclosure for SEC registrants. That proposed rule has suggested that risk factor disclosures should be based on the registrant's own risk identification process (vs. following a generic list).

Other Voluntary Disclosures

Even if the above disclosures are made by companies, it does not mean that a company actively and continuously manages its risks as part of its strategic and operational planning processes. Boards, shareholders, and other stakeholders should want to know more about a company's ERM process. This applies to public and private organizations.

Some companies publicly disclose that they have an ERM process. Other companies disclose that they have a risk committee, CRO, or risk infrastructure. Still others disclose software they are using for ERM. One biotech company discloses key process/operational risks in addition to other risk factors and how those risks fit into ERM. They further disclose how they are measuring and managing that risk.

International Disclosure and Risk Oversight

Other countries have also adopted best practices in risk, corporate governance, and ERM. For example, countries such as Singapore have requirements that the audit committee should understand the ERM framework in place and that the board should ensure an ERM framework and strategy is set, and countries such as South Africa have the King IV Report that lists principles for good governance and says boards should govern risk to support the strategic objectives.

IX. Conclusion

Every year the World Economic Forum reminds us of the changing global risk landscape with risks such as involuntary migration, extreme weather, state collapses, water crises, and so on. On top of a risky world, business leaders face an ever–growing set of emerging risks such as new competition, disruption, innovation, Big Data, the emergence of analytics, the Internet of Things, changes in data privacy laws, automation, artificial intelligence, blockchain, continued cyber risks, and robotic processes. The list seems endless, the risks seem to grow and get more complicated, and the risks seem to move more rapidly. The management accountant, the finance function, the controller, the CFO, and all of leadership find themselves being held more and more accountable for seeing and managing this myriad of risks. Risk competence has become a core competence for business leaders. In fact, not knowing or seeing a risk has become unacceptable and potential grounds for dismissal.

In today's risky world, companies can no longer rely on a silo approach to risk management. An integrated and holistic perspective of all the risks facing the organization is needed. A risk-centric organization does not avoid risks, but rather it knowingly takes risks aligned with its risk appetite. ERM frameworks written by COSO and ISO are globally applicable and adaptable and can be used by organizations of any size. They are principle–based and can help a company better manage and navigate the broad and rapidly changing set of risks.

Integration of ERM with ongoing management activities serves to embed risk management throughout a company. As companies attempt to implement ERM, some best practices (presented in Exhibit 17) can be a valuable reference. ERM is essential in today's business environment, and the goal is still to create, protect, and enhance value.

EXHIBIT 17: 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 represent 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., "Hallmarks of Best-Practice ERM," *Financial Executive,* January/February 2005, p. 38.

Glossary

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

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

Likelihood – An estimate of the chance or probability of a 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 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 narrower level than risk appetite.

Bibliography

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

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

Barton, Thomas L., William G. Shenkir, and Paul L. Walker, Making *Enterprise Risk Management Pay Off,* Financial Executives Research Foundation, Upper Saddle River, N.J., 2001.

Barton, Thomas L., William G. Shenkir, and Paul L. Walker, "Managing Risk: An Enterprise-wide Approach," *Financial Executive,* March-April 2001, pp. 48-51.

Basel Committee on Banking Supervision, *International Convergence of Capital Measurement and Capital Standards, A Revised Framework,* June 2004.

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

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

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

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

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

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

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

COSO, *Enterprise Risk Management—Integrated Framework: Application Techniques,* AICPA, New York, 2004.

COSO, *Enterprise Risk Management—Integrating with Strategy and Performance,* COSO, 2017.

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

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

Deloitte, "Enterprise Risk Management: A 'risk-intelligent' approach," 2015.

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,* The Economist Intelligent Unit, New York, 1995.

Economist Intelligence, *Enterprise Risk Management Implementing New Solutions,* The Economist Intelligent Unit, New York, 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,* IFAC, New York, 1999.

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

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

Hands On, "Risk Management Issues for Privately Held Companies," *ACC Docket,* May 2006, pp. 76-88.

King Committee on Corporate Governance, *King IV Report on Corporate Governance for South-Africa,* Institute of Directors in Southern Africa, 2016.

IEC 31010:2009, *Risk Management—Risk Assessment Techniques,* 2009, International Organization for Standardization.

Institute of Chartered Accountants in England and Wales (ICAEW), *No Surprises: The Case for Better Risk Reporting,* ICAEW, London, 1999.

ISO 31000, *Risk Management—Risk Assessment Techniques,* 2009, International Organization for Standardization.

ISO 31010, *Risk Management—Principles and guidelines,* 2009, International Organization for Standardization.

ISO 31000, *Risk Management,* 2018, International Organization for Standardization.

IMA, "A Global Perspective on Assessing Internal Control over Financial Reporting (ICoFR)," Discussion Draft for Comment, September 2006.

IMA, "IMA Announces Bold Steps to 'Get it Right' on Sarbanes-Oxley Compliance," December 21, 2005.

James Lam & Associates Inc., "Hallmarks of Best-Practice ERM," *Financial Executive,* January/February 2005, p. 38.

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

Kaplan, Robert S., and David P. Norton, "Putting the Balanced Scorecard to Work," *Harvard Business Review,* September-October 1993, pp. 134-147.

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

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

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

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

Miccolis, J.A., K. Hively, and B.W. Merkley, *Enterprise Risk Management: Trends and Emerging Practices,* The Institute of Internal Auditors Research Foundation, Altamonte Springs, Fla., 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, pp. 1-6.

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

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

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

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

Oversight Systems, "The 2006 Oversight Systems Financial Executive Report on Risk Management," 2006.

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

Protiviti, *Guide to Enterprise Risk Management,* 2006.

Protiviti, *Guide to Enterprise Risk Management: Frequently Asked Questions,* 2006.

Protiviti, "Board Perspectives: Risk Oversight: How Mature are Our Risk Management Capabilities," 2015.

Righi, Brandon, and Carol Fox, "2017 Enterprise Risk Management Benchmark Survey," 2017.

RIMS, Risk Maturity Model, 2018, www.rims.org/resources/ERM/Pages/RiskMaturityModel.aspx.

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

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

Shaw, Helen, "The Trouble with COSO," CFO, March 15, 2006, pp. 1-4.

Shenkir, W., and Paul L. Walker, "Enterprise Risk Management and the Strategy-Risk-Focused Organization," *Cost Management,* May-June 2006, pp. 32-38.

Simons, Robert L., "Control in an Age of Empowerment," *Harvard Business Review,* March-April 1995, pp. 80-88.

Simons, Robert L., "How Risky Is Your Company?" *Harvard Business Review,* May-June 1999, pp. 85-94.

Slywotzky, Adrian J., and John Drzik, "Countering the Biggest Risk of All," *Harvard Business Review,* Reprint R0504E, April 2005, pp. 1-12.

Smith, Carl, "Internal Controls," *Strategic Finance,* March 2006, p. 6.

Smith, Wendy K., and Richard S. Tedlow, "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.

Smutniak, John, "Living Dangerously: A Survey of Risk," *The Economist,* January 24, 2004, pp. 1-15.

Standard & Poor's, *Criteria: Assessing Enterprise Risk Management Practices of Financial Institutions: Rating Criteria and Best Practices,* September 22, 2006.

Standard & Poor's, *Insurance Criteria: Refining the Focus of Insurer Enterprise Risk Management Criteria,* June 2, 2006.

Stroh, Patrick, "Enterprise Risk Management at United Health Group," *Strategic Finance,* July 2005, pp. 27-35.

Thornton, Emily, "A Yardstick for Corporate Risk," *Business Week,* August 26, 2002, pp. 106-108.

Treasury Board of Canada Secretariat, *Integrated Risk Management Framework,* 2001.

Treasury Board of Canada Secretariat, *Integrated Risk Management Framework: A Report on Implementation Progress,* 2003.

U.S. Securities and Exchange Commission (SEC), "Commission Guidance Regarding Management's Discussion and Analysis of Financial Condition and Results of Operations," Release No. 33-8350, December 19, 2003.

SEC, "Securities Offering Reform," Release No. 33-8591, December 1, 2005.

Walker, Paul L., "Innovation and ERM: Partners in Managing the Waves of Disruption," IMA and ACCA, 2016.

Walker, Paul L, "Noise to Signals to Business Models—Tools and Challenges for Managing the Risky Waves of Change," Center for Excellence in ERM (at St. John's University) white paper, 2017.

Walker, Paul L., and Mark L. Frigo, "Managing Risk in A Disruptive World," Financial Executives Research Foundation, 2017.

Walker, Paul L., William G. Shenkir, and Thomas L. Barton, *Enterprise Risk Management: Pulling It All Together,* The Institute of Internal Auditors Research Foundation, 2002.

Walker, Paul L., William G. Shenkir, and Thomas L. Barton, "ERM in Practice," *Internal Auditor,* August 2003, pp. 51-55.

Walker, Paul L., William G. Shenkir, and Thomas L. Barton, "Improving Board Risk Oversight through Best Practices," Institute of Internal Auditors, 2012.

Walker, Paul L., William G. Shenkir, and Thomas L. Barton, "A Risk Challenge Culture," IMA and ACCA, 2014.

Walker, Paul L., William G. Shenkir, and C. Stephen Hunn, "Developing Risk Skills: An Investigation of Business Risks and Controls at Prudential Insurance Company of America," *Issues in Accounting Education,* May 2001, pp. 291-304.

World Economic Forum, "The Global Risks Report 2017," 12th Edition.